Technology and Risk Management Policies and Procedures Manual

ACCEPTABLE USE POLICY

OVERVIEW

Purpose and Scope

The purpose of this policy is to identify guidelines for the use of Le Jardin Community Center, technologies and communications systems. This policy establishes a minimum standard that must be upheld and enforced by users of the Organization's technology and communications systems.

The term employee as used in these policies refers to employees (whether full-time, part-time, or limited-term), independent contractors, consultants, and any other user having authorized access to and using any of the Organization's computers or electronic communications resources.

Computer and electronic communications resources include, but are not limited to, host computers, file servers, stand-alone computers, laptops, tablet PCs, printers, fax machines, notebooks, phones, smart phones, online services, e-mail systems, bulletin board systems, blogs owned by staff members where the Organization is discussed, blog comments by staff members regarding the Organization, social networking sites (Facebook®, Instagram®, LinkedIn®, etc.), and all software that is owned, licensed, or operated by Le Jardin Community Center.

Acceptable Use of Organization Property

Use of the Organization's computers and electronic communications technology is for program and business activities of Le Jardin Community Center. These resources shall be used in an honest, ethical, and legal manner that conforms to applicable license agreements, contracts, and policies regarding their intended use. Although incidental and occasional personal use of the Organization's communications systems is permitted, users automatically waive any rights to privacy.

In addition, the information, ideas, concepts and knowledge described, documented, or contained in the Organization's electronic systems are the intellectual property of Le Jardin Community Center. The copying or use of the Organization's intellectual property for personal use or benefit during or after employment (or period of contract or nondisclosure agreement) Le Jardin Community Center is prohibited unless approved in advance by the **Executive Director**

Portions of Le Jardin Community Center information, records, and data are highly sensitive and subject to restrictions imposed by the Health Insurance Portability and Accounting Act of 1996 (HIPAA), the Gramm-Leach-Bliley Act of 1999, and the Sarbanes-Oxley Act of 2002, as well as all other data management restrictions resulting from local, state, federal, and international laws.

All hardware (laptops, computers, monitors, mice, keyboards, tablet PCs, printers, telephones, notebooks, fax machines, walkie talkie, smartphone, hotspot devices, hard drive, etc.) issued by Le Jardin Community Center is the property of the Organization and should be treated as such. Users may not physically alter or attempt repairs on any hardware at any time. Users must report any problems with hardware to the IT Department, **IT Specialist**

GENERAL REQUIREMENTS

The following general rules apply to all personnel that interact with the organization's assets:

- All data, including e-mail and other communications, created by users on Le Jardin Community Center systems remains the property of Le Jardin Community Center.
- Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Reasonableness involves not only following organization policy, but following laws, regulations, and general security good practices.
- Organization personnel will allow authorized individuals within Le Jardin Community Center to monitor equipment, systems, and network traffic as needed.
- The organization has the right to collect and review the contents of any organization owned information asset.
- Le Jardin Community Center reserves the right to audit networks and systems on a periodic basis.

INTERNET AND COMMUNICATIONS

All Internet use, including use of any Internet, Intranet, or Extranet, that is performed on organization equipment or over organization networks falls under the organization domain and must follow the organization policies. All organization systems are to be used for business purposes. However, the organization allows occasional inconsequential personal use of the Internet, provided such use does not interfere with business uses, personnel productivity, or burden the network or the organization's information systems. Use of the Internet or any information systems that are or may be illegal, offensive, or in violation of policies are prohibited.

The following requirements must be followed for all personnel using the Internet on devices owned by the Organization:

- All confidential information sent over external networks by any means must be encrypted with approved organization technology. Certain types of transmissions may require additional controls. Please contact the Technology Department for further guidance.
- The organization may block Internet sites or protocols that the organization deems to be inappropriate or may contain the risk of harmful or malicious programs. A site that is not blocked should not necessarily be considered acceptable. Personnel must immediately leave inappropriate sites they encounter.
- Personnel must not disclose any organization confidential or internal information on external bulletin boards, blogs, Web pages, instant messages, etc., without organization

executive approval. This applies to all social media sites and other similar types of external locations.

- While personnel may comment on information that is not for internal use only or confidential, personnel must also understand their actions are logged and are subject to review. While personnel have the right of free speech, they should remember there is responsibility attached to that right.
- Personnel are prohibited from performing the following actions on devices owned by the Organization:
    - Engaging in any communication that is discriminatory, defamatory, pornographic, obscene, racist, sexist, or that evidences religious bias or is otherwise of a derogatory nature toward any specific person, or toward any race, nationality, gender, marital status, sexual orientation, religion, disability, physical characteristic, or age group.
    - Browsing, downloading, forwarding, and/or printing pornographic, profane, discriminatory, threatening, or otherwise offensive material from any source including, but not limited to, the Internet.
    - Engaging in any communication that is in violation of federal, state, or local laws.
    - Proselytizing or promoting religious beliefs or tenets.
    - Campaigning for or against any candidate for political office or any ballot proposal or issue.
    - Sending, forwarding, redistributing, or replying to chain letters.
    - Using unauthorized passwords to gain access to another user's information or communications on the Organization's systems or elsewhere.
    - Advertising, solicitation, or other commercial, non-programmatic use.
    - Knowingly introducing a computer virus into the communications systems or otherwise knowingly causing damage to the systems.
    - Using the systems in a manner that interferes with normal business functions in any way, including but not limited to, streaming audio from the Internet during business hours, stock tickers, Internet gaming, installing unauthorized software, etc.
    - Excessive personal use of technologies that preempts any business activity or interferes with organizational productivity.
    - Sending e-mail messages under an assumed name or obscuring the origin of an e-mail message sent or received.
    - Employees will not make unauthorized access to vendor sites to inappropriately or illegally utilize information within or from these sites.

CLASSIFICATION AND HANDLING OF INFORMATION

Information Classification Definitions

Each organization department must adopt a three-tier classification system consisting of Public, Internal, and Confidential levels of classification for information.

- Public - Information suitable for release to the public, following approval by authorized organization representatives for general release to the public.
- Internal – Information controlled by the organization that may be made available to all employees and to authorized contractors, consultants, or other third parties but not to the general public because unauthorized external disclosure could cause some damage to the organization or any of its associates (employees, customers, etc.).
- Confidential - Information that, if lost, disclosed, or inappropriately modified could cause significant damage to the organization or any of its associates (employees, customers, donors, etc.). Access to confidential information must be restricted based on the need-to-know principle. Confidential information includes, but is not limited to, information owned by third parties and obtained under contract, such as non-disclosure agreements, sensitive (non-public) information about any individuals, including business customers, vendors and employees, financial data, organization strategies, or other information that is subject to protection under laws, regulations, contractual agreements, and/or company policy.

Information Handling Table

The following table defines the appropriate handling of confidential information for the organization. Also see the applicable policies for expanded information throughout this manual.

STORAGE	***Handling practices related to storage are oriented to provide reasonable physical protection of information, regardless of form, against unauthorized disclosure. This also includes hardware, software, or other mechanisms that would provide access to confidential information.***
Physical Form	Provide controlled physical access and environmental controls for mass storage of information. For example, storing information in a controlled office area or securing the information in a desk or file cabinet.
Electronic Form	Store on authorized information systems only. Data stored on portable computing devices and portable media such as laptops, PDAs, floppies, CDs, smart phones, and USB drives must be encrypted per policy.

SHARING/DISCLOSURE	***Sharing and disclosure practices are primarily aimed at enforcing the need-to-know principle, ensuring that the sensitivity of the information is properly conveyed, and ensuring that third-party arrangements are properly addressed.***
Internal associates, contractors, temporary employees	Information should only be shared with internal employees, contractors, and temporary employees with a business need for the information. Convey classification and handling requirements to recipients.
External business partners	Only disclose to external partners with a business need to know that information and to those that have executed appropriate legal agreements. Convey classification and handling requirements to recipients.
TRANSMISSION	***Controls around the transmission of information are used to ensure that such information receives a level of protection traversing uncontrolled environments commensurate with its sensitivity and criticality.***
Electronic transmission (External-Individual)	Consider implementing management approval for transmission unless using encryption approved by the organization.
Electronic transmission (Fax)	Notify recipient prior to the transmission if recipient's fax machine or information system is located in an unsecured area.
Mail/Delivery (External)	Sealed opaque envelope/packaging using courier, delivery service, international equivalent, or U.S. Postal Service. Packages should be picked up and delivered in a secure location by carrier (e.g., in carriers drop box or other secure location).
RETENTION, DISPOSITION, & DESTRUCTION	***Handling practices around the retention and disposal of information, or devices providing access to such information, help to ensure that business and legal requirements related to information retention are followed and that information released is in an unusable/unreadable form.***
Information retention requirements	As defined by the specific department retention requirements.

Electronic data purging & media destruction	Consider all types of media. Purging, clearing, or destruction must reasonably prevent the reconstruction of the information.
REMOVING INFORMATION FROM COMPANY PREMISES	***Controls around removing information from company premises (e.g., taking work home or to business partner location) are used to ensure that such information receives a level of protection in uncontrolled environments commensurate with its sensitivity and criticality.***
All	Personnel shall employ the same handling restrictions for all information when removed from company premises.

E-MAIL COMMUNICATIONS

The Organization may communicate with its customers, vendors, and clients via e-mail. E-mail is not a secure or private communications mechanism and employees should not treat it that way. Sensitive or confidential information should not be sent via e-mail over the Internet without encryption.

Employees should exercise care in the use of e-mail and in the handling of e-mail attachments. If an e-mail is from someone you do not know, or if you were not expecting an attachment, do not open it; delete it. The user should contact the IT Specialist to report the questionable email and for assistance if there are questions as to the validity of the message and attachment.

The following requirements pertain to the sending and receiving of e-mails, as well as the usage of the organization's e-mail system.

- Personnel may not use the organization's network to send spam, "junk mail," or any unsolicited material to individuals who did not specifically request such material.
- Personnel may not use unauthorized or forged e-mail header information.
- Personnel may not create or forward "chain letters" or "pyramid schemes" of any type using the organization's e-mail system.
- Personnel may not use the organization's e-mail system to send harassing messages, create a hostile work environment, hoaxes, pornographic material, or otherwise perform illegal activities.
- Personnel must use a high degree of caution when opening e-mail attachments received from unknown senders. This is a common vector for virus or malware infection.
- Sensitive or confidential information must be transmitted via a secure messaging solution.
    - Any applicable questions should be directed to the IT Specialist.

- Personnel may make unauthorized copies or backups of their email inbox contents, such as .pst files, without permission of the IT Specialist.

Personnel must delete e-mail messages that are no longer relevant for organization business. Personnel are responsible for using non-e-mail directories for retaining messages and attachments that are needed for an extended period. Personnel must retain e-mails related to known organization litigation and contact organization Human Resources or Legal counsel if they believe they may have any documentation related to a pending or current legal matter of the organization.

DOWNLOADS

Personnel must not access, modify, delete, print, or copy confidential information without a business need. Personnel must not download, install, use, or otherwise make available tools designed to corrupt the confidentiality, integrity, or availability of organization information systems. Personnel must have organization approval to download and use all software on organization assets. All downloaded software must be tested by the Technology Department for acceptable organization use and infrastructure compatibility, as well as an examination of virus and spyware or any malicious code. Software downloaded from the Internet may only be obtained for business purposes. Personnel must request and obtain permission of the IT Specialist to install any software to a device owned by the Organization.

ACKNOWLEDGMENT SIGN-OFF

All organization employees, volunteers, or others utilizing the information systems of Le Jardin Community Center must read and sign an acknowledgment of this policy of entire manual, we include training on the policies each year during pre-service. This is intended to ensure that every employee is aware of the current security practices and ethical responsibilities contained in this policy.

DISCIPLINE FOR NONCOMPLIANCE

Personnel should be aware of potential penalties for noncompliance with organization policy, which may include suspension of certain security privileges, suspension of employment, or termination. Issues with adherence to this policy will be addressed utilizing the organization's approach to disciplinary action and with the assistance of the Human Resources Director.

ASSET INVENTORY

Le Jardin Community Center must maintain an inventory of business and information technology (IT) assets to be used to continue operations in the event IT systems, such as servers and databases, are rendered unavailable due to a systems outage, systems failure or disaster. Inventories of assets must be kept current and be included in any plan documentation.

Asset Identification

Le Jardin Community Center must identify ownership of IT and business assets and must collect the following information for each asset:

- Type and ID number, description of asset, make or manufacturer, model, serial number, and other information that uniquely identifies the asset.
- Physical location of the asset.
- Owner for each IT business asset.
- Any confidential information on the asset.

RISK ASSESSMENT

The Risk Assessment uses various threat scenarios to assist in determining the severity and impact of a disaster Le Jardin Community Center may use existing Information Technology Risk Assessment to cover requirements as long as the assessments have specific data. The goals of the IT Department assessment are to:

- List scenario threats to the organization, including threats to your people, facilities, and IT infrastructure.
- Prioritize potential disasters based upon their severity, which is determined by their impact on operations and the probability of occurrence.
- Identify operational vulnerabilities and weak business processes.
- Determine cost-effective mitigation strategies to reduce the threat probability or impact.

CLOUD SERVICES SECURITY POLICY

OVERVIEW

In addition to overall cybersecurity, Le Jardin Community Center recognizes the need for a Cloud Security Policy to define controls and responsibilities to address the heightened risk of data breaches resulting in loss or compromise, or the operational impact of cyber-attacks on cloud services critical to Organization. As stated in the cybersecurity policy below, the organization must identify the cloud services used, and their criticality based on the data shared with each.

Areas of concern, relating specifically to cloud services risk include the following. Cloud service policy requires controls and validations for each of the points below.

- Acceptable data access controls
    - The organization will validate data access controls and protections meet requirements based on data and systems classification.
- Acceptable Access and Authentication
    - The organization will validate system access and authentication controls and protections meet requirements based on data and systems classification.
        - Role based access based on need-to-know only access
        - Acceptable multi-factor authentication controls
        - Acceptable identity management controls
        - Consideration of transaction level authentication
        - Acceptable identity management audit controls
- Acceptable data backups and media protections
    - The organization will validate system data backups and media protections meet requirements based on data and systems classification and recovery objectives. This includes acceptable data backup audit controls.
- Acceptable solution or service monitoring controls
- Acceptable data life or permanence controls
    - Acceptable data destruction methods and success confirmations
- Acceptable data sovereignty controls
    - The organization will validate system data sovereignty controls meet requirements based on data and systems classification, and any prohibitions for off-shore data residence.
- Acceptable data transportation encryption
- Acceptable resiliency and business continuity and disaster recovery (**BC**/**DR**) controls, plans and test results
    - The organization will validate system resiliency and BC/DR controls, plans and test results meet requirements based on data and systems classification and recovery objectives.

- Acceptable Data Loss Prevention (**DLP**) controls and monitoring
- Acceptable Incident Response plans and test results
    - The organization will validate system Incident Response plans and test results meet requirements based on data and systems classification and data breach response regulatory or lawful requirements, and organization objectives.
- Acceptable remote access controls
- Acceptable multi-tenant access controls
- Acceptable Audit tools for systems performance and control validations
- Acceptable 4th party access and monitoring controls
- Acceptable Off-shore entity access restrictions

CYBERSECURITY POLICY

OVERVIEW

Le Jardin Community Center recognizes the need for a Cybersecurity Policy to define controls and responsibilities to address the heightened risk of data breaches resulting in loss or compromise, or the operational impact of cyber-attacks. The organization's activities particularly impacted by cybersecurity risk include:

- Conduct e-commerce on its website, such as processing donations or event registrations.
- Store and transfer (such as by sending to the cloud) "personally identifiable information," (Common examples of personally identifiable information include: clients' medical information; employee records, including drivers' licenses, addresses, and social security numbers.)
- Collection of information on preferences of patrons, newsletter subscribers, etc.

Cyber Risk Assessment and Remediation

The organization must assess its risk and perform the key steps to implement appropriate protective and detective controls, along with response and recovery processes. The following steps will be taken to address cybersecurity concerns.

- **Step 1 – Risk Assessment:** Begins with taking an inventory of all of the data the organization collects and identify where it is stored. Over time, reduce or limit data collected and retained where ever possible. Diligently destroy data in accordance with the organization's document retention policy to reduce risk.
- **Step 2 – Identify "protected" or "confidential" data:** Know whether the data the organization collects and maintains is covered by federal or state regulations as "personally identifiable information." If so, forty-seven states' laws require nonprofits to inform persons whose "personally identifiable information" is disclosed in a security breach (It does not apply to us), and 31 states have laws that require disposal of such data in certain ways disposal record for our organization). Additionally, the Federal

Trade Commission's Disposal Rule also requires proper disposal of information in consumer reports and records to protect against “unauthorized access to or use of the information.” Protecting personally identifiable information is all about training staff how to collect/store/dispose of and generally protect this data.

- **Step 3 – Drill down on actual risks:** The organization will consider using the (NIST) Cybersecurity Framework (the Windows Framework has to be latest updated), or a comparable tool to help your nonprofit identify risks, and make management decisions to mitigate those risks. The NIST framework is not intended to be a one-size-fits-all approach but to allow organizations to manage cybersecurity risks in a cost-effective way, based on their own environment and needs.
- **Step 4 – Promptly Address Identified Deficiencies:** Control frameworks (as mentioned above) identify testing requirements for validation of expected protections in the form of Controls Audits, Vulnerability Assessments, as well as comprehensive monitoring of the infrastructure and penetration and social engineering tests. Each of these can bring to light issues that must be remediated promptly. The organization will prioritize and promptly address identified deficiencies.

Web Site Risk

The risk is to the nonprofit’s reputation so, on balance, a site takeover does not create the same type of liability risks that other security breaches do, but cleaning up the mess can be time consuming and costly. To managing these risks, the organization will endeavor to keep software updated and being vigilant about usernames and passwords (example: Using “admin” as a user name creates vulnerabilities, say the experts.) Regular maintenance can go a long way towards reducing this and other data security risks.

Cyber Liability Insurance

The organization’s management will assess risk appropriate for the organization’s needs.

DISASTER RECOVERY PLANNING POLICY

OVERVIEW

Le Jardin Community Center recognizes the need for a Disaster Recovery Planning (**DRP**) Policy to define the process for the recovery of IT systems in the event information systems are unavailable are rendered unavailable, such as during systems outages, systems failures or disasters. It is important that executive management be informed of all Le Jardin Community Center BCP policy statements, plans, and tests. This policy sets out overall policy objectives, but Le Jardin Community Center must develop the detail necessary to fully implement the policy requirements. Goals of the DRP program include:

- Minimizing the disruption of service to Le Jardin Community Center.
- Recovering data.
- Facilitating the prompt resumption of services.

Disaster Recovery Planning (DRP) policy requirements include:

- Establishing overall authority and responsibility in the development, implementation and maintenance of the DRP.
- Creating guidance for determining business impact levels.
- Outlining strategies for recovery efforts.
- Establishing requirements for periodic testing of the plans.

Authority

Executive management must approve the selection of a DRP Coordinator (IT). This role coordinates the DRP effort and moves the planning through all phases to completion and testing. To assist DRP Coordinator, a DRP Committee should be formed from the owners of all IT systems that would need to be recovered related to the disaster recovery plan. The Committee will assist in the design, development, drafting, and finalization of a formal disaster recovery plan for each IT system, provide ongoing management processes, oversee the implementation of the program, and serve in a leadership role during a disaster. The DRP Committee should coordinate with the Information Technology Committee to effectively manage technical assets and resources.
IT Department responsibilities include:

- Determine any needed changes to the program, report them to management, and assist departmental implementation.
- Review, evaluate, and change the plan as necessary to accommodate comments and recommendations provided by critical departments.

- Update procedures to relocate at any off-site locations and maintain the necessary supplies for emergencies.
- Oversee media backup and storage off-site to enable reconstruction of all critical files used by Le Jardin Community Center.

ASSET INVENTORY

Le Jardin Community Center must maintain an inventory of information technology (IT) assets consisting of physical assets (hardware, network devices, etc.) and logical assets (data, software, licensing, and applications). Inventories of assets must be kept current and be included in any plan documentation.

Asset Identification

Le Jardin Community Center must identify ownership of IT assets and must collect the following information for each asset:

- Type and ID number, description of asset, make or manufacturer, model, serial number, and other information that uniquely identifies the asset.
- Location, physical or logical, of the asset and the information classification of each asset.
- Relationships and dependencies between physical and logical assets, including which hardware is required for each software application.
- Security processes or controls (including access controls, backups, etc.) associated with each asset.
- Data owner for each asset.
- Any confidential information on the asset.

BUSINESS IMPACT ANALYSIS

Le Jardin Community Center must create a Business Impact Analysis (BIA). The BIA determines the potential revenue loss related to non-recovery of critical business processes and identifies the departments or critical processes necessary to the recovery of the organization.

The following should be identified:

- Potential threats, the impact of each threat, and its likelihood.
- Critical business processes and information systems.
- Maximum allowable downtime a critical system can incur.
- Priorities for critical systems.
- Internal and external customers to define which business processes are the most important to the organization's survival.
- Financial and operational considerations, regulatory requirements, and legal obligations.
- Organizational reputation and operational efficiency.

Prioritization

Prioritization of systems for IT department involves creating system criticality levels. Factors that must be considered when determining information or system criticality include processing importance of hardware, system software, applications programs, and human involvement in operations.

There are three levels of priority for IT recovery:

- Critical Levels: Level 1, Level 2, Level 3
    - Critical Level 1 = restore immediately (within 24 hours). This is highly critical to the survival of the organization. Immediate recovery is required to prevent substantial loss to or degradation of operations.
    - Critical Level 2 = restore within 48 hours. This is moderately critical to the survival of the organization. Further delay could potentially raise this to Critical Level 1.
    - Critical Level 3 = restore within 72 hours. This is important to the survival of the organization. To delay further could raise the criticality level due to increase in volume or passage of time.

- Non-critical: Level 1, Level 2
    - Non-critical Level 1 = restore within 7 days. This is important to the effectiveness or efficiency of the management of the organization.
    - Non-critical Level 2 = restore within 21 days. This is not immediately important to the effectiveness or efficiency of the management of the organization but is still relevant to restore at some point.

Recovery Time Objectives

Recovery Time Objective (RTO) is the time during which a recovery must become effective before an outage compromises the ability of Le Jardin Community Center to achieve its critical business objectives or survival. If the time is not met, a disruption in operations could have a significant impact.

Recovery Point Objectives

The Recovery Point Objective (RPO) is the time after the initial disaster when the organization plans to recover data. The RPO represents the point in time, prior to such an event or incident, to which lost data can be recovered (given the most recent backup copy of the data). The RPO is a function of the extent to which the interruption disrupts normal operations and the amount of financial loss per unit of time as a result of the disaster. These factors in turn depend on the affected equipment and application(s). Both of these numbers represent key targets that must be set by critical departments. These targets may drive the technology and implementation choices for business resumption services, backup, recovery, archival services, and recovery facilities and procedures.

Setting the RPO assists the organization in the following ways:

- RPO targets help define the organization's risk awareness and requirements.
- RPO assists in selecting or developing the appropriate recovery technologies and strategies.
- RPO provides testing benchmarks.
- RPO creates the basis for a data recovery service level agreement (SLA).

OPERATIONAL REQUIREMENTS

Backup Use

The organization's Data Backup Plan must establish procedures to create and maintain retrievable exact copies of critical electronic information and related technology components that are necessary for recovery activities. Backup processing plans for a disaster must include:

- Operating procedures for backup of organization data.
- Requirements for data retention.
- Detail on how the organization will use offsite storage and how the backup media will be retrieved.

Backup Requirements

The following operational procedures should be described in the IT Plan to adequately address back up organization information and recovery in the case of an emergency.

A. Backup Timing – How often does the organization need to back up for recovery?

- Daily incremental backups.
- Weekly full backups.
- Monthly full backups.
- Daily replication of data.

B. Data Storage

- Database shadowing - Database information is duplicated by being simultaneously written to another server.
- Electronic vaulting - Batch process that makes a copy of backup data to an offsite location.
- Remote journaling - Live data transfers are passed to the offsite location with full synchronization of both sites.

Technology

The organization must determine the configurations of computer equipment required for recovery. This includes mainframes, servers, personal computers, peripherals, LANs, switches, routers, and other data communication equipment. The organization must also decide how fast it needs to utilize its technical resources after any disaster. Systems specifications should be kept current to assist in implementing organization technology at an alternate location if necessary. Specifications include documentation of:

- Computer hardware.
- Logical/physical system designs.
- Configuration diagrams.
- Systems software.
- Application software.
- Data files.
- User documentation.
- Report forms/templates.

Alternate Facility Options for Technical Requirements

Based on the Business Impact Analysis, the organization may use an alternate facility equipped as follows:

- Mirrored site - This is a type of file synchronization where a site holds an exact copy of the original data set. The benefits of a mirrored site include no downtime, a fully equipped site, and actively running identical processes. This requires the use of redundant technologies such as Redundant Array of Inexpensive Disks (RAID), clustering, and backup power supplies
- Hot site - A hot site is a full or partial duplicate for a primary IT operation, including complete computer systems and near-real-time backups for systems, applications, and data. Critical operations can be up in minutes to hours. This is similar to the mirror site except data/staff may be lessened, and it may only hold the most critical operational data.
- Warm site - This is an alternative business recovery facility equipped, unlike a hot site, with only minimally necessary computer hardware and software, communications equipment, power supply, and environmental support equipment. Technology recovery could take days to weeks, depending on how it is equipped and made ready for operations.

TESTING

The DRP must be tested regularly to ensure that the plan is up to date and effective. Such tests should also ensure that all members of the recovery team and other relevant staff are aware of the plans. The ability of the DRP to be effective in emergency situations can only be assessed if rigorous testing is carried out in realistic conditions/scenarios, which means simulating conditions which would be applicable in an actual emergency. It is also important that the persons who would be responsible for those activities in a crisis should carry out the tests.

Test Plan

The fundamental goal of the test plan is to carry out all the steps documented in the DRP. However, not all tests will cover all areas of the plan. The test plan must permit flexibility for testing without modifying the actual plan. The goal of the test plan is to identify the sections of the plan to test, identify any additional tasks required for testing outside of the plan, and identify any tasks in the plan that cannot be completed due the test environment. The test plan should analyze the performance of the test by rating the outcome of the activities performed during the test. Rating each task should show areas where the DRP did well and areas requiring attention. The results of the test should be reported to executive management.

DATA BACKUP POLICY

OVERVIEW

Data Backup is required for servers, network storage devices, and other media that contain critical or sensitive information and/or programs. The policy is designed to protect data in the organization to ensure it is not lost and that it can be recovered due to unanticipated failure, such as equipment failure, intentional destruction of data, or disaster.

The Information Technology Department must enforce the policy for Le Jardin Community Center. An Information Technology employee may be designated to perform regular backups of systems and data. The designated person is responsible for ensuring backups are performed and testing the ability to restore data from backups on a weekly basis.

ONSITE BACKUP

Onsite backup is performed daily, with incremental backups occurring nightly Sunday through Friday. A full backup is performed on Saturday night. The media must be labeled (this is a folder labeled with the backup date. Le Jardin Community Center critical or confidential data must be backed up via the network media procedures, not using local drives or individual media. Examples of backup media include backups to an external hard drive or backups to a server located on site.

EMPLOYEE LOCAL BACKUP

Employees using standard office software, such as MS Office Suite, must save Le Jardin Community Center critical or confidential data files to the file server so that these data files may be backed up automatically for recovery purposes. For any data files saved to locations other than the approved networked servers and devices, users must understand that there is no other maintained backup system and data may be erased or deleted. Employees must also protect those non-network storage locations appropriately for the classification of information stored on them.

Data Replication

With a data replication solution, no physical backup media are used. A copy of data is saved to a remote location, such as in the cloud or at an alternate site, either on a synchronous or asynchronous basis. With a synchronous solution, all new data or modified data is immediately saved over to the remote location. With an asynchronous solution, the data is copied over to the remote site within a period of time, such as daily or weekly.

Offsite Backup

A separate set of media must be created each week combining all backup days for that week. Incremental backups performed Sunday through Friday shall be removed daily and taken offsite. Five generations of post-processing backups will be maintained offsite. Examples of offsite backup media include tapes or external hard drives that are transported offsite after collection of backup data.

Monthly Backups

Every month, the last full backup performed shall be archived as that month's backup. The monthly backup will be stored at the offsite location.

Data Backed Up

The following servers will be included in full and incremental backups:

- File server.
- Primary and secondary domain controllers.
- Production database server.
- Network management server.
- Other servers containing critical or confidential information.

DIGITAL EQUIPMENT DISPOSAL POLICY

OVERVIEW

Any piece of digital equipment must be reliably disposed of. This involves erasure and/or destruction either internally by approved Information Technology Specialist or externally by an approved third-party. Le Jardin Community Center prohibits employees and others from discarding digital equipment with any non-public information in the regular garbage to mitigate the risk of accidental disclosure. All employees have a responsibility to ensure that digital equipment is returned to the appropriate department for proper erasure or disposal.

Digital equipment includes all Organization-owned storage devices which contain software programs, computer code, and/or Organizational confidential or non-public information. Digital equipment includes, but is not limited to, all digital storage devices such as desktop workstations, laptops, servers, notebooks, handheld computers or tablets, internal and external hard drives, and all external data storage devices such as disks, SANs, optical media (e.g., DVD, CD), magnetic media (e.g., tapes, diskettes), and non-volatile electronic media (e.g., memory sticks) and backup tapes.

DIGITAL EQUIPMENT DISPOSAL HANDLING REQUIREMENTS

Erasure and Destruction

Erasure – The organization may use erasure as a non-destructive means of removing information from equipment. This can be done when the equipment or assets can be reused internally within the organization. Erasure of information on equipment or assets must be performed to eliminate the risk of information being viewed or reconstructed by someone who does not have a need to know or the right to view that information.

Destruction – When equipment will not be reused internally within the organization or if the asset is being sold or donated with the data storage device intact, complete and permanent elimination of information must be accomplished.

1. Organization-owned digital equipment must have all organization data and licensed software reliably erased from the device prior to its transfer out of Organization control. Control includes the time until an approved IT Department has erased and/or destroyed the equipment.

2. IT Department that perform equipment destruction must supply Le Jardin Community Center with documentation attesting to the erasure or destruction. Internally approved methods for erasure and equipment destruction must use approved procedures following industry best practices for the type of media. Information Technology employee must ensure that procedures consistent with security best practices are followed for the reliable removal of licensed software and confidential data.

3. Prior to erasure or destruction of digital equipment, an ‘Equipment Disposal Form’ must be completed listing the reason for disposal, date, tag #, description, model #, and serial #. If an external vendor performs the erasure or destruction, the form should have a ‘Certificate of Destruction’ attached from the vendor upon destruction completion.

Employee or Third Party Purchase and Donation of Digital Equipment

Digital equipment which is working, but reached the end of its useful life to Le Jardin Community Center may be made available for purchase by employees, third party or donated to approve entities. This decision will be determined by the Information Technology and Finance departments. Any digital equipment that is made available for purchase or donation must be securely erased by approved methods. If made available for purchase, a lottery system will be used to determine who has the opportunity to purchase available digital equipment. Finance and Information Technology will determine an appropriate cost for each item. All purchases are final. No warranty or support will be provided with any equipment sold.

DOCUMENT RETENTION POLICY

OVERVIEW

Le Jardin Community Center retains records as required by law and destroys them when appropriate. The destruction of records must be approved by the CFO/COO and logged into the Organization's Destroyed Records Log.

Within an organization, it is often necessary for employees to retain electronic documents for a period of time due to regulations or the need to access archival information. This period of time may vary depending on the type of document and the required need for storage. Electronic documents can include files such as e-mail messages, Web formatted files, audio and video files, text files, PDF documents, and vendor specific as in Microsoft Office or other formatted files. This policy applies to all employees who create electronic documents and any Le Jardin Community Center work or personal related documents that are stored on workstations, servers, network (including cloud based), personal digital assistants (PDA), mobile devices, or any other devices within Le Jardin Community Center technology environment.

The Le Jardin Community Center has implemented this policy for the following reasons:

- To comply with regulation and litigation requirements as mandated by law.
- To conserve storage space on the network, servers, and workstations.
- To assist in maintaining optimal performance of Le Jardin Community Center network.
- To reduce discrepancies amongst different document versioning.

POLICY

Document Types and Guidelines

The following are the types of electronic documents and files covered under this policy. Other formats may be added as necessary.

When the Laptop has been returned to IT department, it will be delete and restore to factory settings, (Any documents, files, picture, video, etc. must be delete or saved by peripheral drive, External hard drive, pen drive)

- E-mail Messages - All e-mail messages, from both internal and external sources, are to be deleted after one year (It just could be apply to regular employees not to Executive board or other level. Employees should by all means possible keep the majority of their e-mails work related and minimize the number of personal messages.
- Web formatted files—All Web formatted files saved on the network or on users' workstations should be deleted by employees after one year.

- Text/formatted files/PDFs—Quarterly reviews of all text/formatted/PDF files (e.g., Microsoft Word documents) will be conducted by employees where any outdated or unnecessary deemed documents will be deleted at that time.
- Audio and video files—any work-related audio and video files (e.g., MP3s, WMVs) will be retained on the network or user's workstation as deemed appropriate by the employee. Any files downloaded for personal use should not be stored on any network share and should be deleted from workstations as necessary to allow the device to function properly. Employees will adhere to Le Jardin Community Center acceptable use policy when downloading audio and/or video files for personal and/or work-related use.
- Spreadsheets— Due to the nature of spreadsheets for financial functions (e.g., budgeting purposes), these stored documents will not be automatically deleted from network shares. Spreadsheets should be stored on appropriate shared network drives, where retention guidelines are enforced depending on the specific use of the document. Before deleting any spreadsheets on the network in use by multiple departments, check with both management and contacts in each department that accesses these documents.
- PowerPoint presentations—Because of wide use of these documents within Le Jardin Community Center, employees are encouraged to store PowerPoint presentations on the network to encourage collaboration between various departments and employees. All PowerPoint presentations should be reviewed on an annual basis and deleted if no longer deemed necessary by Le Jardin Community Center.

Exception for Investigations

In connection with any ongoing or anticipated investigation into allegations of violations of federal laws or regulations, provisions of government awards, or violations of the Organization's Code of Conduct, the following exceptions are made to the preceding scheduled retention and/or destruction of records:

1. All records related to the subject of the investigation or allegation shall be exempt from any scheduled record destruction.
2. The term "records" shall also apply to any electronically stored record (e.g., documents stored on computers, e-mail messages), which shall also be protected from destruction.

INFORMATION SECURITY CONTROLS POLICY

OVERVIEW

Le Jardin Community Center uses physical and system controls to protect information and systems from security threats. Threats to the organization can include theft; unauthorized access; and use, disclosure, disruption, modification, or destruction of information. Le Jardin Community Center has a responsibility to its staff, volunteers, and clients to use reasonable defenses against attempts to gain unauthorized access, such as an attack attempting to exploit a vulnerability. This policy addresses the requirements in many of the critical controls in the organization's operations.

AUTHENTICATION AND PASSWORDS

Authentication

Authentication is the verification of the user's identity by a system. This is based on the presentation or delivery of unique credentials to that system. The unique credentials can be in the form of various factors, i.e., something the user knows, something the user has, or something the user is. This can take the form of tokens, biometrics (fingerprints), or shared secrets (such as passwords). More than one form can be used, and when two or more are deployed, it is called multi-factor authentication. This is generally stronger than any single factor authentication method. Authentication contributes to the confidentiality of data and the accountability of actions performed on the system by verifying the unique identity of the system user.

It is the policy of the Organization to employ, maintain, and monitor various authentication methods appropriate to the level of risk based upon the following general criteria:

- Assess the risk of loss of the information and select the authentication methods based on that risk associated with the particular application, system, or services;

- Determine whether multi-factor authentication is appropriate or feasible for all applications, taking into account that multi-factor authentication may be necessary to protect the organization's information; and

- Encrypting the transmission and storage of authentication methods (e.g., passwords, personal identification numbers, and any biometric identifiers).

Employee Authentication

All employees are required and expected to safeguard information by protecting passwords and other methods of authentication. Under no circumstances are passwords shared with anyone including family members, friends, co-workers managers, or the Information Technology

Department. Employees are responsible for all activity performed with their accounts and passwords. Employees are forbidden from performing any activity with passwords belonging to other users. If it becomes necessary for the organization to require knowledge of an employee's personal password for any reason, the employee will be required to change the password prior to network logon.

Employees should refrain from using the same passwords on organization accounts as for other non-organization accounts. When possible, refrain from using the same password for multiple organization accounts as well. Contact the Help Desk or Information Technology Department to change your password if you suspect that it has been compromised.

Passwords

General Password Construction Guidelines

Passwords are used for various purposes at Le Jardin Community Center. Passwords are the initial defense in the protection of Le Jardin Community Center information from unauthorized access. Uses include: user level accounts, e-mail accounts, Web accounts, screen saver protection, and voicemail passwords. All Le Jardin Community Center staff and volunteers using the organization's systems should be aware of how to select strong passwords. Passwords on all Le Jardin Community Center systems are subject to the following:

1. Users are responsible for safeguarding their system passwords.
2. Users should not leave their computers unattended without logging off. Le Jardin Community Center has configured workstations to lock after 15 minutes of inactivity.
3. If a user suspects that the secrecy of the user's password has been compromised, the user should report this to the Specialist of Information Technology immediately and initiate a password change request.
4. Passwords should not be displayed or concealed in the employee's work area.
5. Passwords will adhere to the following complexity guidelines:
    a. Password may not contain all or part of the user's account name. They should not be a dictionary word or any other word connected to the user, such as the name of a user's family member.
    b. Password contains characters from three of the following four categories:
        1) English uppercase characters (A…Z)
        2) English lowercase characters (a…z)
        3) Base 10 digits (0…9)
        4) Non-alphanumeric (exclamation point [!], dollar sign [$], pound sign [#], percent sign [%], etc.)

Examples of poor or weak passwords are those with the following characteristics:

- The password contains less than eight characters.
- The password is a word found in a dictionary (English or foreign).

- The password is a common usage word such as:
    - Word or number patterns like abcde, 12345, etc.
    - Birthdays and other personal information such as addresses and phone numbers.
    - Names of family, pets, friends, etc.
    - Computer phrases and names or commands.
    - The words "ORGANIZATION," or a form of the city name where the organization is located.
- Any of the above spelled backwards.
- Any of the above preceded or followed by a digit (e.g., secret1, 1secret).

NOTE: Do not use either of these examples as passwords!

Password Protection Standards

Users should not use the same password for Le Jardin Community Center accounts as for other non-Organization access (e.g., personal ISP account, banking sites, benefits administration, etc.). Where possible, do not use the same password for different Le Jardin Community Center access needs.

Do not share Le Jardin Community Center passwords with anyone. All passwords are to be treated as sensitive, confidential information.

Here is a list of password related “DON’Ts:

- Don’t use the "Remember Password" feature of applications or your Web browser
- Don't reveal a password over the phone to ANYONE, including someone purportedly from the Organization’s Information Technology Department.
- Don't reveal a password to your supervisor.
- Don't reveal a password to coworkers when you go on vacation.
- Don't reveal a password in an e-mail message.
- Don't talk about a password in front of others.

If someone requests a password, refer them to this policy or have them call someone in the Information Technology Department.

Please do not write passwords down and store them anywhere in your office or work location. Do not store passwords in a file or document on ANY computer system without encryption.

If your account or password is suspected to have been compromised in any way, report the incident to the Information Technology Department immediately and change the password immediately.

The Information Technology Department may perform password cracking or guessing as an evaluation of Le Jardin Community Center passwords. This could be done on either a periodic

or random basis. If a password is guessed or cracked during one of these evaluations, the user will be required to change it.

NETWORK AND SYSTEM MANAGEMENT

Access Overview

The Organization's goal is to allow access by staff, volunteers, and others approved to use the organization's systems and to disallow access to all others. Authorized individuals may be employees, vendors, contractors, customers, or visitors. Access will be provided only to individuals whose identity is established, with levels limited to the minimum required for organizational purposes.

Access Rights Administration

Access rights must be administered in the following areas:

- A process to add new users to the system;
- Assigning users and devices role-based access, allowing them to perform their duties;
- Updating access rights based on personnel or system changes to add, delete or modify authorized user access to operating systems, applications, directories, files and specific types of information;
- An authentication process to identify the user during subsequent activities; and
- Periodically reviewing users' access rights for key applications and the network, preferably on an annual basis.

The new user set-up process must establish the user's identity and organizational needs for information and systems. For some systems, the assignment of access rights is performed by the department manager, following network access configuration by the Information Technology Department. The assignment of rights will be set according to the employee's role or group membership and managed by pre-established authorizations for that group.

Since access rights do not automatically expire or update, it is the responsibility of the organization's management to conduct periodic updating and review of access rights on the system. Updating occurs when an individual's organizational needs for system use changes. Many job changes can result in an increase or decrease of access rights. Job events that would trigger a removal of access rights include transfers, resignations, and terminations. It is the responsibility of the Information Technology staff to closely monitor and remove the access rights for users who have remote access privileges, access to confidential information, and perform administration functions for the Organization's systems.

Default Accounts

Default user accounts associated with new hardware or software must be disabled or the password associated with the account changed as standard operating procedure. Access to these default accounts must be monitored and reviewed. Anonymous access accounts must be disabled for all systems that allow access to or store confidential information.

Logging and Monitoring Reports

The Organization's logging and monitoring reports contain host and network data gathering for review, analysis, and storage. Host data is gathered and recorded in logs and includes detailing of performance and system events, including behavior that may indicate an intrusion. Security logs will be retained, allowing the organization to identify security issues and enforce accountability. Security event logs may include operating system access, privileged access, and creation of privileged accounts, configuration changes, and application access attempts (both successful and unsuccessful). Confidential applications may require their own logging of significant events.

Network Logging and Monitoring

The Organization's networks are designed to support a monitoring process that includes:

- Network traffic policies and configuration that addresses the communications between computers or groups of computers;
- Log storage and protection from removal or tampering

It is the responsibility of the Information Technology Department, in addition to any third-party vendor contracted for this purpose, to administer the activity monitoring processes to detect any potential breach in security.

Intrusion Detection/Prevention

Le Jardin Community Center may implement a Network Intrusion Detection and Prevention System, if feasible. These systems perform as an access control mechanism, allowing for access based on an analysis of packet headers and packet contents. The functions of the Network Intrusion Detection and Prevention System are:

- Monitoring and analysis of user and system activity
- Auditing of system configurations and vulnerabilities
- Assessing the integrity of critical system and data files
- Statistical analysis of activity patterns based on the matching to known attacks
- Abnormal activity analysis
- Operating system audit
- Identifying potential threats and responding to them swiftly

Intrusion Detection/Prevention Requirements

If implemented, the Network Intrusion Detection and Prevention System requirements will include:

- All intrusion detection logs must be kept for a minimum of 90 days.
- All systems accessible from the Internet or by the public must operate IT-approved active intrusion detection software.
- All systems segregated in a separate network area between the firewall and the network must operate IT-approved active intrusion detection software.
- All intrusion detection systems must be checked on a regular basis, often performed daily, and their logs reviewed.

System Quarantine

Quarantining a system or device is a measure that protects the network from potentially malicious code or actions. If a system or device connecting to a security domain does not meet approved standards, it will be placed in a restricted part of the network until it does meet those standards or is permanently removed from the network.

Patch Management

Patches are updates to commercially developed software to correct identified flaws that otherwise can create security or performance vulnerabilities on servers, desktops, laptops, or other organization information device. Effective patch management will assist the organization in mitigating the risks associated with software vulnerabilities and in ensuring that the security and availability of computer systems is not compromised.

Patch management process requirements include:

- New devices must be patched to the current patch level, as defined by the operating system vendor, prior to the system being connected to any production network.
- Patches will be applied as soon as possible following appropriate testing of the patches by the Information Technology Department.
- All networked devices managed by the organization will be patched with vendor-provided operating system security patches.

Patch Responsibilities

The Information Technology Department Network Administrator (Administrator), in collaboration with any System Owners or Custodians, will stay current on organization hardware and software issues and/or shortcomings. The Administrator will be responsible for monitoring and identifying updates relevant to Le Jardin Community Center critical operating systems. The potential

impact of the patch should be determined and an appropriate test plan developed prior to implementation. All patches must be tested and approved prior to release. Testing should occur on a selected computer or subset of the population of computers before any patch is released to all production computers. New patches should be tested in a controlled environment that mimics the infrastructure of the production environment before patches are applied.

Patch Approval

Before approving patches, the Administrator(s) should evaluate:

- The vulnerability addressed by the patch.
- What programs are affected by the patch?
- What previous patches are required or what system update is required?
- What may be broken by the patch?
- How to undo the patch.
- Whether data backup has been applied prior to applying the patch.
- All patches approved for client computers or applied to client computers should be documented.

FIREWALLS AND VIRUS PROTECTION

Firewalls

Firewalls are employed by Le Jardin Community Center to protect the network from unauthorized access. Dedicated firewalls must be used on all Internet connections where inbound access is allowed. Firewalls can be separate devices, a component on a larger device, such as a router, or software-based. Firewalls protect systems that contain confidential data within the internal network.

The Organization will implement and maintain appropriate firewalls by:

- Defining the type of allowed or disallowed traffic coming into and going out of Le Jardin Community Center network. This will be based on the assumption that all traffic not expressly allowed is denied.
- Managing and updating the Organization's firewall, which may include collaboration with a third-party service provider.
- Detailing which protocols and applications can traverse the firewall and under what exact circumstances this can occur.
- Detailing the firewall and security architecture.
- Listing the type of firewall(s) deployed.
- Monitoring firewall traffic.
- Coordinating with security monitoring and incident response procedures.

- Ensuring that a regular external audit is performed of a firewall's configuration and testing of the firewall's effectiveness is performed.

Firewall Backup

Before any major changes or alterations to the firewall policies are performed, a complete backup of the firewall configuration files and operating system will be performed. This backup will be stored securely and available in the event a restoration is required. This firewall rule set should be backed up whenever a configuration change is applied.

These events may initiate an in-depth analysis of log file activity:

- A virus has infected a machine within Le Jardin Community Center Network.
- A daily log file analysis exposes any questionable activity.
- A new Internet exploit has been discovered that directly relates to an application or service used by Le Jardin Community Center
- An employee of Le Jardin Community Center or a subcontractor is suspected of suspicious activity in relation to computer usage or released due to any suspicious computer activity.

Physical Security of the Firewall

To ensure maximum security for the Organization network, the firewall itself will be located in a cabinet that is protected by a locked door or within a room where access is restricted to Information Technology Department staff only. The firewall should be protected from external electrical surges via a surge protector designed to protect an Ethernet cable segment. The firewall will be plugged into an uninterruptible power source (UPS).

IT Events that can trigger a policy rule review include:

- New applications incorporated in the Organization network.
- If an application is phased out or upgraded.
- A new software or firmware release has become available for the firewall itself.
- Any information security incident.
- Any changes in corporate policy.
- Any changes that affect the way the firewall is administered, maintained, or monitored.

Types of reviews include:

- Configuration review to ensure that current rules are consistent with policy deployed in firewall.
- Periodic reviews from a system audit and vulnerability assessment of production and backup firewall devices.

Virus Protection

All Le Jardin Community Center employees must protect against the threat of viruses. When an infected file is opened from a computer connected to the organization's network, the virus can spread throughout the network and may do considerable damage. Viruses can enter Le Jardin Community Center network through:

- E-mail - As attachments, documents, links or spreadsheets can carry viruses in macros, or the virus may be disguised as pictures, jokes, etc. Once some viruses are opened, they automatically e-mail themselves, and the sender may not know his or her computer is infected at all.
- USB Drive, DVD, CD, Zip disk, or other media - Viruses can also spread by many types of storage devices or media; as with e-mail attachments, a virus may hide within a legitimate document or spreadsheet or simply be disguised as another type of file.
- Software downloaded from the Internet - Downloading software from the Internet can also be a method of infection. As with other types of transmissions, the virus could hide within a legitimate document, spreadsheet, or other type of file.
- Instant messaging and social media application attachments - Similar to e-mail attachments, instant messaging and social media applications may provide a method of virus infection through file attachments.
- Clicking a link connected to malware while browsing the internet. Once a user clicks a malicious link, malware could be installed unbeknownst to the user.

Virus Examination

The organization must examine corporate assets for viruses using multiple methods:

- Scanning Internet traffic - All Internet traffic coming to and going from the organization's network must pass through servers and other network devices.
- E-mail server review - E-mail must be scanned for viruses and/or malware. This scan should evaluate all e-mail as it enters the server and scan all e-mail before it leaves the domain.
- Routinely updating virus definitions - If a new virus definition file is available, the virus scanning software will be updated, this is performed at a scheduled time.

Responding to and Reporting a Virus

Even though all Internet traffic is scanned for viruses and all files on the organization's servers are scanned, the possibility still exists that a new or well-hidden virus could find its way to an employee's workstation, and if not properly handled, it could infect Le Jardin Community Center network.

Employees should perform the following safeguards to help the organization stay free of viruses:

- If a file you receive contains macros that you are unsure about, disable the macros.
- Never download freeware or shareware from the Internet.
- Do not open unexpected e-mail attachments, even from co-workers.
- Never open an e-mail or instant messaging attachment from an unknown or suspicious source.
- Avoid clicking links on websites, especially if the website is not highly reputable or if it is unknown to the user.

Notify the Information Technology Department of Suspicious Files

If you receive a suspicious file or e-mail attachment, do not open it. Call the Information Technology Department and inform them that you have received a suspicious file. They will explain how to handle the file.

OPERATING SYSTEM

The Organization maintains controls to protect operating systems and system utilities. Access to operating systems and system utilities is limited to appropriate technology staff and selected third-party service providers. Access control security software is used to restrict access to operating systems and applications.

System Hardening

System hardening and locking down unnecessary processes improves Le Jardin Community Center information security and further restricts potential unauthorized access to information. Unnecessary processes will be stopped and all agency infrastructure devices, including servers, firewalls, router switches, and other components will be hardened and locked down.

System Hardening Processes

The organization will lock down servers prior to network connection. Steps may include some or all of the following:

- Based on the server's purpose, generate a list of all services that will be required to run on the server.
- Patch the server with the latest patches and patch all services running on the server. Turn off any services that the Network Administrator will not require.
- Perform a port scan on the server.
- Perform a vulnerability assessment scan of the server.
- Patch or fix any vulnerability found.
- Remove any unnecessary programs, services, and drivers from the server.
- Be sure file share and file permissions are as tight as possible.

- Disable or change the password of any default accounts on the server or related to any operating services.
- Enable audit logging to log any unauthorized access.
- Be sure all passwords used to access the system or used by services on the system meet minimum requirements, including length and complexity parameters.
- Be sure all users and services have minimum required rights and do not have rights to items not needed.
- Set security parameters on all software. This can include where anti-virus programs will scan, how often it will scan, and how often it will get virus definition updates for the software provider.
- Take additional account management security steps including:
  - Disable the guest account.
  - Rename default administrator accounts.
  - Set accounts for minimum possible access.
  - Be sure all accounts have passwords meeting minimum complexity and length rules.
- Test the server to be sure all approved services are operating properly.
- Remove any unnecessary network protocols.
- Uninstall any unnecessary software that may have vulnerabilities that may allow unauthorized access.

The organization will perform the following processes prior to attaching a new computer to the network:

- Develop a systems build CD/DVD with necessary drivers and applications copied to it.
- Establish a password for the administrator account.
- Remove all advertising, promotional, evaluation, and/or non-standard applications.
- Remove any antivirus software pre-installed on the system.
- Install Le Jardin Community Center approved antivirus software.
- Turn on software firewall.
- Install printers and other peripherals.
- Create a new user account with password.
- Turn off unnecessary Windows services.
- Establish a system restore point if the operating system is capable of this step.

REMOTE ACCESS

Employee Remote Access

Le Jardin Community Center employees may be granted remote access to organizational information, hardware, software, communication systems, and the Internet in accordance with their job responsibilities and subject to the human resources policies of Le Jardin Community Center. The IT Specialist will approve all remote access request before they are granted. This access is to be used for the purpose of performing job-related duties in an appropriate,

responsible manner in accordance with organization acceptable user policies and procedures and in compliance with applicable laws and regulations.

Remote Access Acceptable Use

Hardware devices, software programs, and network systems provided by the organization for remote access are to be used only for creating, researching, and processing organization-related materials. By using the organization's hardware, software, and network systems, the employee assumes personal responsibility for their appropriate use.

At no time should any employee provide login or passwords to organization assets to anyone, not even family members.

Employee Remote Access

Organization vendors requiring remote access to organization systems must have written approval for the access. The organization will, for each vendor remote access situation, have the authority to grant and remove access. The following requirements for remote access sessions must be adhered to:

- No more than two simultaneous sessions are allowed.
- Any password or personal identification number (PIN) will be at least 6 characters in length.
- Sessions will disconnect after 15 minutes of inactivity.
- The duration of a single session can be unlimited time.
- Employee must have unique user accounts assigned to them for any system that they will be accessing.
- The gateway should have access control lists in place.

PORTABLE MEDIA

Portable media, including laptops, smart phones, iPads, netbooks, tablet PCs, personal digital assistants (PDAs), smartphones, and other storage devices, are vulnerable to both physical damage and theft. Both the value of the portable media and the organization information on the media must be protected.

Laptops

Employees granted the use of organization-owned laptop computers should protect such equipment and ensure the security of confidential information. Employees should:

- Keep the laptop in possession and within sight whenever possible. Be especially careful in public places such as airports, libraries, or other public venues.

- Lock the laptop up, or store it completely out of sight when you are not using it, preferably in a filing cabinet or safe.
- Carry and store the laptop in a padded laptop computer bag or strong briefcase to reduce the chance of damage.
- Do not download, install, or use unauthorised software programs on the laptop.
- Never leave a laptop visibly unattended in a vehicle.
- If the laptop is lost or stolen, notify the police immediately and inform the Information Technology Department as soon as possible.
- If traveling, the laptop must remain in the possession of the user as hand luggage at all times.

Mobile Devices

Storage of confidential organization files or information on a mobile device is not permitted without specific approval. Mobile devices include (but are not limited to) smart phones, iPads, netbooks, tablet PCs and tablet PCs that perform similar functions as laptops but may not have all the protections as a laptop. This does not apply to e-mail stored on the device for viewing only. Organization data viewed or stored on mobile devices is the property of the organization. Upon employee termination, users must remove all organization data from any device. The organization reserves the right to verify that Organization data is removed from the device.

Storage Media

All portable storage devices or media, such as CD-R/Ws, DVD-R/Ws, diskettes, external/portable hard drives, and USB memory sticks (jump drives) that contain data or software must be stored in a physically secure location when not in use. The Information Technology Specialist must approve removal of any “storage media” from the premise of the Organization and all contents must be encrypted.

INFORMATION SECURITY INCIDENT RESPONSE

Purpose

An information security incident occurs after the unauthorized disclosure or use of the organization’s confidential information, including loss of data confidentiality, disruption of data integrity, or disruption or denial of service. Le jardin community center employees have a duty to follow the requirements of the policy in the event of any potential or confirmed information security incidents. The organization must take steps to detect, contain, and resolve incidents.

The organization will observe any regulatory or funder guidance to ensure protection not only to proprietary systems and data, but also to any sensitive information entrusted to us by our customers.

All security breaches must be addressed through the completion of the Incident Response Tracking Form. All employees must report suspected information security breaches to Le Jardin Community Center management immediately.

Incident Response Team

The organization has created an incident response team to address the identification, notification, remediation, public relations, client relations, and risk mitigation steps required to minimize impact to the organization and the organization's clients. The team should include members from the Information Technology Department and various business departments, such as Operations, Legal, Communications, and any others who may be able to provide assistance in the case of an incident. Any management member must report potential incidents to the Incident Response Team management as soon as possible. The team will examine the potential level of impact. The types of impact include:

- Loss of data.
- Loss of funding or revenue.
- Loss of confidence in the organization by clients, the general public, or funders.

Incident Detection

Le Jardin Community Center places the security and confidentiality of information entrusted to it in a position of paramount importance. In order to detect potential or actual breaches to information security, Le Jardin Community Center has implemented the controls and safeguards. The Incident Response Team will be responsible for ensuring that the appropriate response procedures are followed. The team will use knowledgeable employees or consultants to determine the scope of the incident. Establishing the scope of the incident includes determining what organization confidential information systems and types of customer information could have been compromised.

If the incident involved unauthorized access to or use of confidential information, the team will determine internal and external notification requirements in compliance with regulatory and stakeholder requirements. The team must document all steps taken to determine the nature of an incident, list all compromised information systems and customer records, and record dates and contact information for external agencies notified of the breach.

Detection steps include, but are not limited to, the following:

- Determine if an incident has occurred and the extent of the incident.
- Notify appropriate personnel.
- Select immediate response communication.
- Assume control of the incident and involve appropriate personnel, as conditions require.
- Assess risk.
- Evaluate options.

- Implement triage.
- Document.
- Preserve evidence for forensics purposes.

Incident Containment

As soon as possible, the Incident Response Team will work to contain the breach and mitigate further damage. Final decision regarding incident containment will be made by the team leader and the Executive Director. Containment efforts may involve utilizing a forensic services vendor or law enforcement assistance, shutting down or isolating compromised systems or networks, terminating negligent or malicious employees or vendors, and changing parameters, procedures, and policies to eliminate weaknesses which led to the incident. Steps taken to contain the incident and the elimination of underlying weaknesses should be documented on the Incident Response Tracking Form.

Containment steps include, but are not limited to, the following:

- Contain the breach as soon as possible by segregating any affected systems from the rest of the network.
- Verify containment has been effective.
- Collect as much accurate and timely information as possible.
- Preserve evidence as collected.
- Protect the rights of clients, employees, and others, as established by law, regulations, and policies.
- Establish and adhere to controls for the proper collection and handling of evidence.
- Initiate a chain of custody of evidence.
- Minimize service interruptions within the organization.
- Document all actions and results thoroughly.

Incident Response Tracking Form Filing

The organization must complete an Incident Response Tracking Form as soon as possible. If the incident appears to be ongoing, the organization will also notify local law enforcement as soon as possible in an attempt to apprehend the unauthorized intruders. The form must be used to document the process throughout the incident. The form will be filed electronically for two years on a backed up organization server.

Client Notification

The Incident Response Team will be responsible for determining if clients should be notified about information security breaches after considering applicable federal, state, and local laws, regulatory guidance, funder requirements, and impact to customer data. If, at the conclusion of a reasonable investigation, the organization determines that misuse of client information has occurred or is reasonably possible that misuse will occur, then client notification will take place.

Client notice must conform to all regulatory requirements, but may include the following items:

- A description of the incident.
- The type of information exposed to unauthorized access.
- Steps taken by the organization to protect clients from further unauthorized access.
- A telephone number clients can call for information and assistance.
- A reminder to clients to remain vigilant over the next 12 to 24 months and report suspected identity theft incidents to the organization.

Incident Resolution

In no case should a compromised system, Web page, or application be returned to normal operation without the approval of a member of senior management and the Information Technology Department. After the incident has been contained, the Incident Response Team will discuss ways to improve the incident response process, ensure that applicable steps, notifications, and event tracking have been formally completed, and to notify senior management about the incident and its resolution. The information security risk assessment and incident response programs should be updated to address lessons learned and to revise applicable sections.

Types of Incidents

Incidents have been classified into low, medium, or high levels, depending on the severity.

Low-Level IT incidents are the least severe and include:

- Computer viruses/worms (depending on impact to the organization).
- Theft of personal password.
- Misuse of computer equipment.
- Suspected sharing of customer accounts.
- Unsuccessful scans/probes.
- Unintentional routine computer actions.

Medium-Level IT incidents are more serious and include:

- Download of unauthorized software (depending on impact to organization).
- Unfriendly employee termination with attempted logon by terminated employee.
- Computer viruses/worms (depending on impact to the organization).
- Violation of access privileges.
- Personal theft related to a computer incident (less than $10,000).
- Illegal building access.
- Property destruction related to a computer incident (less than $10,000).
- Unauthorized use of a system for processing or storing organization data.

High-Level IT incidents are the most serious and include:

- Any violation of law resulting that could result in a felony conviction or a misdemeanor conviction punishable by incarceration.
- Suspected or actual computer break-in.
- Download of unauthorized software (depending on impact to organization).
- Denial of service attacks.
- Illegal distribution of inappropriate content, such as content that contains the following material (not an exhaustive list); pornography/child pornography, racism, sexism, violence.
- Computer malware, such as viruses, worms or ransomware, (depending on impact to the organization).
- Unauthorized use of a system for processing or storing customer or other confidential data.
- Illegal software download and/or installation.
- Changes to system hardware, firmware, or software without the system owner's authorization.
- File exploitation/manipulation.
- Property destruction related to a computer incident (more than $10,000).
- Personal theft related to a computer incident (more than $10,000).

WIRELESS NETWORK SECURITY

Wireless Networks Connecting to the Organization

The following requirements must be adhered to for wireless use:

- Wireless hardware will be limited to devices approved by the Information Technology Department.
- All wireless networks must enable Wi-Fi Protected Access 2 (WPA2) and Advanced Encryption Standard (AES) technology for encryption and authentication.
- All wireless networking adaptors must be provided, installed, and maintained by the Information Technology Department.
- Network bridging (split tunneling) must be disabled on all devices that use wireless technologies.

Procedures

In accordance with the standards set forth under federal and state statutory requirements (hereafter referred to as regulatory requirements), Le Jardin Community Center is committed to ensuring the confidentiality, integrity, and availability of all protected health information and

corporate internal and confidential data (hereafter all three will be referred to as covered information) it creates, receives, maintains, and/or transmits.

To comply with regulatory requirements, Le Jardin Community Center has established internal corporate governance for safeguarding the confidentiality, integrity, and availability of covered information the workforce creates, receives, maintains, or transmits. Le Jardin Community Center must have in place appropriate administrative, technical, and physical safeguards to protect covered information.

Key Definitions

Asset: A major application, general support system, high impact program, physical plant, mission critical system, personnel, equipment, or a logically related group of systems.

Compensating Controls: Safeguards or countermeasures used to mitigate the severity or impact of a vulnerability (i.e. risk) to covered information. Compensating controls can be technical or non-technical in nature.

Continuous Monitoring: Is the process and technology used to detect compliance and risk issues associated with an organization's environment. The environment consists of people, processes, and systems working together to support efficient and effective operations. Through continuous monitoring of the operations and controls, weak or poorly designed or implemented controls can be corrected or replaced – thus enhancing the organization's operational risk profile.

Covered Information: General term used to define all data requiring specific administrative, physical, technical and operational controls to ensure the confidentiality, integrity and availability of information in accordance with regulatory requirements and corporate governance. At a minimum this would include corporate internal or confidential data.

Designated Approving Authority (DAA): Ssenior official (i.e. CEO) within the organization, or his/her designated representative with the authority to formally assume responsibility for accepting risk on behalf of the organization. The DAA grants or denies authority to accept risk based on his or her knowledge of the needs of the business, and the recommendations of the IT Specialist.

Electronic Protected Health Information (ePHI): Any individually identifiable health information protected by HIPAA that is created and transmitted by or stored in electronic form.

Guest Account: An account assigned to a guest/visitor of the organization hosting a wireless network for which the account is being provided access to.

Individually Identifiable Health Information: That information that is a subset of health information, including demographic information collected from an individual, and is created or

received by a health care provider, health plan, employer, or health care clearinghouse; and relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and identifies the individual; or with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Non-Technical Controls: are management and operational controls such as security policies, standards and procedures that address personnel, physical, and environmental security risks.

Plan of Action and Milestones (POAM): Also referred to as a corrective action plan, is a tool that identifies tasks that need to be accomplished to meet the requirements of a risk acceptance decision (i.e. approval to operate). It details resources required to accomplish the elements of the plan, any milestones in meeting the task, and scheduled completion dates for the milestones. The purpose of the POA&M is to assist Le Jardin Community Center with identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for security weaknesses found in programs and systems.

Protected Health Information (PHI): Individually identifiable health information (i.e. paper based) that is created by or received by the organization, including demographic information that identifies an individual, or provides a reasonable basis to believe the information can be used to identify an individual, and relates to:

- Past, present or future physical or mental health or condition of an individual.
- The provision of health care to an individual.
- The past, present, or future payment for the provision of health care to an individual.

Remediation: The act or process of correcting a fault, finding or deficiency.

Risk: The level of impact on organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of occurrence.

Risk Assessment/Analysis: Risk assessment and analysis are often used interchangeably. Within this policy, the terms are used as follows:

- Risk Assessment - The process of identifying and prioritizing risks to the confidentiality, integrity and availability of covered information. Risk assessments are meant to identify risks, not analyze or remediate risks.
- Risk analysis - Is the analysis of risks identified during a risk assessment, determining the likelihood of occurrence and impact, then deciding what controls will be implemented to reduce the risk to an acceptable level. A thorough and accurate risk analysis will consider all relevant losses that would be expected if security measures were not in place or not performing as expected, including loss or damage of data, corrupted data systems, and anticipated ramifications of such losses or damage.

Risk Management: The process of managing risks to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, resulting from the operation or use of an information system, and includes: (1) the conduct of a risk analysis; (2) the implementation of a risk mitigation strategy; (3) employment of techniques and procedures for the continuous monitoring of the security state of the information system; and (4) documenting the overall risk management program.

Risk Mitigation: Prioritizing, evaluating, and implementing the appropriate risk-reducing controls/countermeasures recommended from the risk management process. The risk mitigation process includes cost-benefit analysis.

Risk Monitoring: Maintaining ongoing awareness of an organization's risk environment, risk management program, and associated activities to support risk decisions.

Risk Tolerance: The level of risk and Le Jardin Community Center is willing to assume in order to achieve a potential desired result.

Technical Controls: Are the controls that are incorporated into system hardware and software (e.g. access controls, encryption, integrity, audit controls, non-repudiation)

Threat: Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

Threat Assessment: Process of formally evaluating the degree of threat to an information system, covered information, or the organization and describing the nature of the threat.

Vulnerability: Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

Workforce: Means employees, volunteers, trainees, consultants, contractors and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity.

Le Jardin Community Center's IT Specialist is responsible for ensuring that both business and guest wireless networks supported by the organization are properly managed and secure. The IT Specialist is responsible for, but not limited to the following:

- Maintaining and enforcement of this policy
- Overseeing compliance with this policy and managing wireless security risks in accordance with the organization's "Information Security Risk Management" and "Vulnerability Management" policies/procedures.
- Defining and documenting configuration management requirements.

- Incident management
- Define access control requirements

Information Technology (IT) is responsible for maintaining the wireless network environment and for implementing the security controls as defined by the IT Specialist and in this policy/procedure. The IT department is responsible for, but not limited to the following:

- Support and maintain wireless infrastructure.
- Monitoring performance and security of wireless networks.
- Assisting the IT Specialist with incident management responsibilities.
- Implementing and maintaining secure configuration requirements as defined by the IT Specialist.
- Implement and manage access control as defined by the IT Specialist.
- Provide wireless network metrics as required by the IT Specialist.
- Conduct periodic site surveys to detect unauthorized or rogue access points. Immediately report unauthorized/rogue access points to the IT Specialist.
- Survey public areas around the organization to detect weak wireless connectivity or interference from other networks.

Wireless Network Access

Scheduler Wireless Internet Access

The wireless access (Business or guest) are going to be to the next following hours:

Monday – Sunday 24 Hours

.

Business wireless network

Access to the business wireless network will be based on role and job responsibility (i.e. need to have). Access to the business wireless network will not be given to personally owned devices unless approved by the IT Specialist and a risk analysis has been performed. If approved, personally owned devices must comply with the “Personally Owned Device Use in the Workplace” policy/procedure.

Access to the business wireless network will follow the same process as required for access to Le Jardin Community Center’s systems/applications, and requires manager approval. Access management requirements are defined in the “Information Access Management” policy.

Guest wireless network

Provided all requirements are implemented for guest wireless configuration and infrastructure segmentation (as defined in this policy), unauthenticated access to the guest wireless is allowed. The guest wireless network “will not” be used to transmit covered information.

Users accessing the guest wireless network will be prompted to read and Terms of Use Agreement, for which they will have to accept by clicking a tab that says they have read and understand the requirements for use of Le Jardin Community Center’s guest wireless network. Users will be prompted to read/accept every 24 hour period. Terms of Use Agreement language will be defined by Le Jardin Community Center’s general counsel who will ensure that the agreement contains the appropriate language and does not violate any federal or statutory requirements.

Guest wireless access will be limited to only Internet access.

Audit and Monitoring Wireless Activity

Business wireless network

Auditing and monitoring wireless activity will follow the same policy/procedure and processes as defined in the “Audit & Monitoring Endpoint Activity” policy.

In addition to what is required under Le Jardin Community Center’s vulnerability management program, the business wireless network will be continually monitored for the following:

- Authorized and unauthorized users/devices attempting or accessing the network
- Known vulnerabilities and current patch levels.
- Malicious or suspicious activity such as denial of service attacks, rogue access points, virus patterns, failed access attempts, attempts to change or circumvent security requirements, etc.
- Failed and successful authentication.
- Date, time and user identification for all successful or unsuccessful access attempts

Guest wireless network

The guest wireless network activity does not need to be “actively” monitored. Activity that will be captured in the audit logs are as follows:

- Date, time and device identification at time of access
- Malicious activity that could result in the guest network failing
- Excessive bandwidth use

Wireless Network/Device Security Requirements

Business wireless network

At a minimum, the business wireless network will be configured as follows:

- All activity will be traceable to an individual (i.e. workforce member).
- Broadcasting of the Service Set Identifier (SSID) will be disabled.
- Locate access points to reduce signal bleed into unauthorized or unprotected locations (e.g. outside of the building, parking lot, etc.)
- Rename the default SSID to something unique and not easily guessable.
- Multiple wireless networks will have their own unique SSID.
- Implement WPA2 encryption (EAP-TLS or PEAP authentication). Open authentication "is not" allowed under any circumstances. All other encryption (i.e. WEP, WPA) are not authorized unless a formal risk analysis has been performed and the identified risks have been accepted by Le Jardin Community Center's designated approving authority.
- Implement media access control (MAC) address access control or some other form of authorized user identification.
- Network management traffic destined for access points will be over a dedicated wired subnet and secure protocols (e.g. SSL, SSH, SNMPv3, etc.) will be used.
- Password (end-user and administrative) composition and management for the business wireless network will follow the same criteria for Le Jardin Community Center passwords, as defined by the "Identification & Authentication" "Secure Configuration Management" policies.
- Default passwords for wireless infrastructure components will be changed before being placed into production, to comply with internal password policy requirements.
- Disable all non-essential and insecure protocols.

Client Devices

Client devices will be configured as follows:

- Mobile devices must be in compliance with Le Jardin Community Center's "Mobile Device Computing" policy.
- Personally owned devices approved for use in the workplace must be in compliance with Le Jardin Community Center's "Personally Owned Device Use in the Workplace" policy.
- Disable peer-to-peer/ad hoc networking.
- Enable personal firewall (when appropriate and feasible)
- Block split tunnels on VPNs
- Block exposure to client ports
- Allow only one Wi-Fi connection manager active at a time
- Disable local file sharing
- Restrict the ability to connect to the wireless and wired networks simultaneously

Network Infrastructure

The business wireless network will have its own dedicated firewall. When feasible and warranted (based on a formal risk analysis) an Intrusion Detection System or Intrusion Prevention System (IDS/IPS) system will be implemented for the business wireless network.

Guest wireless network

The guest wireless network will be logically segmented (separated) from the business wireless network, to include a VLAN environment. The guest wireless network will be configured as follows:

- All activity will be traceable to a device.
- Broadcasting of the Service Set Identifier (SSID) will be enabled.
- Locate access points to reduce signal bleed beyond the organization's campus (e.g. outside of the building, parking lot, etc.)
- Rename the default SSID to something easily identifiable such as **Lejardin Guest**.
- Default passwords for guest wireless infrastructure components will be changed before being placed into production, to comply with internal password policy requirements. Configuration requirements pertaining to the management of the guest wireless network are the same as the business wireless network.
- Blocking inappropriate Internet content (i.e. pornography).
- Guests are responsible for providing their own end-to-end encryption.

Physical Security Requirements

At a minimum, the business wireless network will be physically separated (i.e. segmented) from the wired network.

Wireless device management system will be physically secured in a data closet or other means that restricts tampering and unauthorized access. Wireless access points will be secured in a manner to prevent tampering.

Guest wireless network

Le Jardin Community Center's guest wireless network will be physically separated from the business wireless network.

Home Wireless Networks

For workforce members who are allowed to work from home and work will involve access to covered information, every attempt will be made to ensure that the home user is made aware of their responsibility to secure their home wireless network. Home wireless network use for

covered information will be addressed in a formal risk analysis by the IT Specialist before allowing use.

Documentation Requirements

Business and guest wireless networks will be documented and maintained for future reference (e.g. audits, assessments, disaster recovery, etc.). At a minimum, documentation will include the following:

- Wireless network infrastructure diagram that shows location of all devices, access points, etc.
- Wireless network component inventory.
- Security attributes and configuration standard.

Applicability

All employees, volunteers, trainees, consultants, contractors and other persons (i.e. workforce) who are responsible for managing and/or maintaining Le Jardin Community Center's wireless security, who work Le Jardin Community Center, are under the direct control of Le Jardin Community Center, whether or not they are directly compensated by Le Jardin Community Center.

CHANGE MANAGEMENT

Le Jardin Community Center has an organized, systematic approach to change management. This process is designed to provide a standardized method in which changes to information resources are requested, approved, and tested prior to installation or implementation. The purpose is to ensure that all steps have been completed, the implementation is carefully planned, and a schedule for implementation is carefully coordinated with all other activities within the organization. Change management procedures apply to all major changes and updates to the organization's systems or infrastructure.

Change Procedure Implementation

Changes to the Organization's information resources may arise due to the following circumstances:

- Acquisition of new hardware and/or software.
- New or modifications to existing policies and procedures.
- Changes in operational schedules, such as hours of availability.
- Hardware and/or software upgrades (patch management when required).
- Periodic maintenance of systems and software.
- Changes or modifications to the Organization's infrastructure or environmental changes.
- User requests.

SOFTWARE INSTALLATION

All new software and applications will be assessed by the Information Technology Department for any potential security impact to the organization. A security assessment, including an assessment of data security levels, media the data will travel over, a risk evaluation, and determination of system requirements will be performed. Identified risks will be mitigated, using plans which will mitigate the most serious security risks from software or application installation. All installations implementations require review and approval by the Technology Committee and the Information Technology Department. Under no circumstances should the overall security of the network be seriously compromised for the benefit of any project.

A software installation checklist must track the following:

- Software type (new/existing) purchased or developed internally/externally.
- Internal software risk assessment.
- Availability of test sample of software for review.
- Completion of software testing.
- Compatibility with other systems and applications.
- Purchase order approval status if externally purchased.
- Communication with department prior to installation.
- Installation of software.

SOFTWARE LICENSING

Le Jardin Community Center will ensure that all software is appropriately licensed and will keep current records of all software licenses. The Information Technology Manager is responsible for periodically reviewing the software inventory to ensure compliance with software license agreements.

INFORMATION SECURITY RESPONSIBILITIES POLICY

OVERVIEW

It is the responsibility of Le Jardin Community Center's executive management, Information Technology Specialist to support and implement the directives of the organization's Information Technology and Security Program. Each role within Le Jardin Community Center has different responsibilities and each individual is to be held accountable for his or her actions. The organization must provide role accountability, this requires clear lines of reporting, clear communication of expectations, and the appropriate use of authority to assist the organization.

RESPONSIBILITIES

Responsibility Objectives

It is the responsibility of Le Jardin Community Center to meet information technology and information security objectives and reduce risks across Le Jardin Community Center. The following are the primary objectives for the organization's policies and controls, around which responsibilities are defined:

1. Availability. Le Jardin Community Center must have confidence that systems will be available to meet organization business requirements. Availability includes allowing authorized users prompt access to information. Control objectives of availability include protection against intentional or accidental attempts to deny authorized users access to information or systems.

2. Integrity of Data or Systems. Systems and data integrity involves making sure information has not been altered in an unauthorized manner. Le Jardin Community Center must ensure that systems are free from unauthorized manipulation that will compromise accuracy, completeness, and reliability.

3. Confidentiality of Data or Systems. Le Jardin Community Center must implement controls to protect the data and systems that contain sensitive or critical data from external or unauthorized exposure. Confidentiality controls include protecting information of Le Jardin Community Center, customers, and other third parties as necessary against unauthorized access or use.

4. Accountability. Accountability involves the ability to record and trace systems and user actions from the originator to end source. Accountability controls support non-repudiation, deterrence, intrusion prevention, security monitoring, recovery, and legal admissibility of records.

5. Assurance. Le Jardin Community Center must have assurance that systems provide the intended functionality while preventing unauthorized actions. Assurance indicates confidence that technical and operational security measures work as intended.

Information Technology/Network Manager

The Information Technology/Network Manager is responsible for implementing the technical requirements of the information technology and information security program. The manager is responsible for communicating technology and information security requirements to staff. The manager must oversee and perform an annual review of the information systems authentication and access rights of personnel.

IT Specialist

The IT Specialist must oversee the creation of adequate controls to protect the confidentiality, integrity, and availability of Le Jardin Community Center's information. IT Specialist duties include the development and review of information security policies, standards, and procedures across the Le Jardin Community Center. The IT Specialist is responsible for providing guidance and direction to the information security program, for determining appropriate controls to reduce risk to an acceptable level, monitoring and responding to information security alerts, and handling information security incidents. The IT Specialist must monitor compliance with the information security program, maintaining effective security risk management and create security awareness programs.

Personnel

All personnel are responsible for reading, understanding, and complying with Le Jardin Community Center technology and information security policy, regardless of whether security controls on information systems enforce policy. All personnel are responsible for their own use of information assets, as well as any equipment or other assets they have been issued. Personnel are responsible for reporting incidents according to the appropriate procedures for their level of responsibility. Security weaknesses and software malfunctions must be reported to management as appropriate. Additional personnel responsibilities are contained throughout the policies, including the Le Jardin Community Center Acceptable Use Policy.

INFORMATION SECURITY RISK MANAGEMENT POLICY

OVERVIEW

Le Jardin Community Center's information security risk management program is a critical function designed to improve the security posture and maturity of the organization. Le Jardin Community Center must understand its risks to be able to reduce its risks. The risk management procedures involve:

- Risk identification.
- Risk measurement.
- Risk control.
- Risk monitoring.

Le Jardin Community Center's risk must be evaluated against common best practice administrative, technical, and physical safeguards and specific additional industry-specific requirements. Examples of IT risk management frameworks include ITIL and COBIT Le Jardin Community Center's information security objectives must include appropriate and formalized mitigation or acceptance of risk based on risk assessment results. The following common information security principles must apply to any risk management strategy:

1. Availability. Le Jardin Community Center must have confidence that systems will be available to meet Le Jardin Community Center business requirements. Availability includes allowing authorized users prompt access to information. Control objectives of availability include protection against intentional or accidental attempts to deny authorized users access to information or systems.
2. Integrity of Data or Systems. System and data integrity involves making sure information has not been altered in an unauthorized manner. Le Jardin Community Center must ensure that systems are free from unauthorized manipulation that will compromise accuracy, completeness, and reliability.
3. Confidentiality of Data or Systems. Le Jardin Community Center against unauthorized access or use.
4. Accountability. Accountability involves the ability to record and trace systems and user actions from the originator to end source. Accountability controls support nonrepudiation, deterrence, intrusion prevention, security monitoring, recovery, and legal admissibility of records.
5. Assurance. Le Jardin Community Center must have assurance that systems provide the intended functionality while preventing unauthorized actions. Assurance indicates confidence that technical and operational security measures work as intended.

POLICY

Risk Assessment

Le Jardin Community Center should perform an annual Information Security Risk Assessment. The assessment must:

- Gather data regarding the information and technology assets of Le Jardin Community Center, including threats and vulnerabilities to those assets.
- Analyze the likelihood, impact, and possible damage from the known threats and vulnerabilities to their assets.
- Understand and document the initial or inherent risk to Le Jardin Community Center prior to controls.
- Evaluate the control effectiveness of existing administrative, technical, and physical security controls and processes.
- Determine remaining or residual risk after control placement.

Le Jardin Community Center must perform the following activities as a result of a risk assessment:

- Prioritize the risks based on the threats, vulnerabilities, and residual risks to determine the appropriate level of ongoing monitoring, training, controls, and assurance necessary for effective mitigation.
- Assign responsibility for any corrective or mitigating activities.
- Perform timely follow-up activities to examine whether mitigation has been completed.
- Report to executive management on the results of the risk assessment and activities to reduce overall Le Jardin Community Center risk.

Risk Assessment Process

Le Jardin Community Center's Information Security Risk Assessment process must include the following elements:

Risk Identification

Le Jardin Community Center's risk assessment must use current documentation of Le Jardin Community Center's operating and business processes to create a risk identification matrix. This information includes both technical and non-technical information that may contribute to Le Jardin Community Center's information security posture. The risk assessment identification phase must include information and information systems to be protected (both paper and electronic). Information and systems that must be included in the assessment involve paper and electronic systems and physical components used to access, store, transmit, protect, and dispose of information.

Risk Measurement and Risk Analysis

The following must be completed to effectively measure and analyze all of the identified risk information:

1. Assess Criticality. Le Jardin Community Center assesses the criticality of the various information systems based on their function, the classification of data, and the business value of data they store, transmit, or protect.

2. Assess Threats and Vulnerabilities. Le Jardin Community Center must assess potential threats and vulnerabilities of its information and information systems. The threat and vulnerability evaluation lists reasonable threats and vulnerabilities, understanding that not every threat and vulnerability can be known, but that common and likely threats and vulnerabilities can be documented. The assessment must determine which threats or vulnerabilities deserve priority attention relative to the value of the information or information systems being protected.

3. Analyze Threats. Le Jardin Community Center must analyze the likelihood, impact, and damage of different threats. The damage to the organization should be measured relative to the loss of Le Jardin Community Center's:

    - Availability, integrity, confidentiality, accountability and assurance of information or information systems.
    - Reputation, transaction capability, compliance, strategic direction, or financial earnings.
    - Person-work quotient hours lost.
    - Time to repair or replace people, systems, or facilities.

Risk Control

Le Jardin Community Center must evaluate the control effectiveness of information protections and information systems and applications. The Organization must identify current administrative, technical, and physical controls and any additional controls that will mitigate the impact or likelihood of each identified threat exploiting a specific vulnerability.

Risk Rating Assignment

Le Jardin Community Center must assign an appropriate risk rating to all information and information systems after completing the analysis of information and information systems. The Organization uses a "High," "Medium," or "Low" risk rating to show both initial, or inherent, risk and for remaining residual risk. The final residual risk rating is assigned in relation to the level of exposure and the threat likelihood, taking into consideration the adequacy of related internal controls.

Risk Monitoring

It is the responsibility of the Information Technology Committee and the IT Specialist to monitor risk mitigation activities to ensure identified mitigation activities are complete or in process. Ongoing monitoring ensures that Le Jardin Community Center's risk reduction process is continuous instead of a one-time or annual event. Le Jardin Community Center must create specific mitigation plans for any residual "High" risks. The Organization should create mitigation or risk acceptance plans for any residual "Medium" risks. Key elements of this process include:

- Prioritization of risks for mitigation.
- Mitigation or corrective action plans.
- Clear assignment of responsibilities and accountability.
- Management reporting.

Prioritization

Prioritization of risks must take into account the following to determine which risks have highest priority:

- Potential damage.
- Technology Strategy.
- Budget.
- Business continuity planning.
- Disaster recovery planning
- Policies.
- Control feasibility.
- Staffing and expertise.
- Insurance.

The prioritization should take into account the risk assessment rating to determine Le Jardin Community Center has reduced the threat risk to an acceptable level or if further mitigation should be considered. The level of remaining/residual risk should drive the initial prioritization controls, training, and testing, but additional factors may also influence the priority order. Final decisions about the acceptance of high or medium risks must be made by executive management on an annual basis or prior to major changes, but with full knowledge of Le Jardin Community Center acceptance risk.

OPERATIONS POLICY

MANUAL/OPERATING PROCEDURES

Each department within Le Jardin Community Center must have complete and job relevant operations manuals and operating procedures. These help to ensure employees are able to understand and meet all job requirements. Operations manuals should address policy requirements for incident response and emergency situations in the department. Manuals and procedures must be readily available for use by personnel. The department must appropriately train all personnel on standard operating procedures and any security requirements that are unique to the department.

Standard operating procedures should list procedure names and describe what the procedure goal or intention is. Procedures may need to integrate with Service Level Agreement levels. The operations service expectations must be formally defined, including delivery expectations and support functions related to the procedure. Operations risk levels should be assessed, understood, accepted or mitigated, and documented. Operations risk should define severity levels and how a failure would impact other systems, products, or procedures and may include the estimated time of resolution. The procedure may provide the expected time to complete the procedure, the department responsible for performing the procedure tasks, plus any dependencies or other procedures that are integrated or have touch points on the procedure.

SEGREGATION OF DUTIES

Segregation of duties is an operational goal where job responsibilities and procedures between different personnel are divided such that no individual has control over all phases of a critical process. The segregation of duties should prevent a single individual from having complete control over all sensitive phases of a process where information or systems could be compromised. Segregation of duties is important to the protection of information and systems because it:

- Increases the likelihood that innocent errors or irregularities are detected by co-workers in a timely manner in the normal course of business.
- Makes deliberate fraud or malicious acts difficult without cooperation between two or more people.
- Creates an environment where no single individual has control over multiple key phases of transactions or operations.
- Reduces damage that can be caused by a single individual due to management oversight over operational activities.

Duty Categories

The following describe the categories of responsibilities into which individual operational duties can be grouped:

- Authorization - Authorization is the process of reviewing and approving transactions or operations involving Le Jardin Community Center information assets. Key words that can indicate that a duty belongs in this category include approve, grant, and certify.
- Collection/Creation - Collection and creation include entry of information into a system, as well as the creation of new information. Key words that can indicate that a duty belongs in this category include submit, request, and initiate.
- Custody - Custody is the possession, management, or control of assets, including Le Jardin Community Center's information assets. Key words that can indicate that a duty belongs in this category include hold, manage, and administer.
- Reconciliation - Reconciliation includes the verification of processing or recording of transactions of information assets to ensure that all transactions are valid, accurate, authorized, and recorded on a timely basis. Words that can indicate that a duty belongs in this category include review, assess, compare, audit, and validate.

Duty Category Conflicts

The following provide some samples of potential conflicts that can arise when the same individual has multiple duties creating a situation for system or information compromise:

- System development or certain technology staff having access or performing updates to production systems. (Creation + Authorization + Custody).
- An individual who submits a system change request also having sole approval of the access request. (Authorization + Creation).
- Network administrator who has "modify" privileges over logs and also audits event logs. (Custody + Reconciliation).
- An individual who creates and updates system access and also approves access requests. (Authorization + Reconciliation).
- A manager who can submit a purchase order and approve the purchase orders. (Creation + Custody).
- An individual who submits a timesheet and can audit their own timesheets. (Creation + Reconciliation).
- An individual who can authorize the release of funds and write checks on the same account. (Authorization + Custody).

Organization Department Responsibilities

The following lists the department responsibilities for determining whether conflicts on separation of duties are occurring:

- A department must perform an analysis to determine whether an individual, or a group of individuals, will be responsible for more than one of the duty categories when handling any confidential information asset or executing an operation on an information asset containing confidential information.

- The department must determine whether the responsibilities related to information assets and related processes should be separated based on classification, impact, and business criticality.
- Where separation of duties should be implemented but is not possible, the department should assess the resulting risk and any compensating controls. If compensating controls cannot be implemented, executive management must formally accept the lack of separation of duties risk.
- The department must create and maintain documents describing how separation of duties will be performed and how the duties will mitigate risk.
- The department must review the access rights of any role where separation of duties is an issue and make sure access is granted based on minimal need-to-know practices.
- The department review and validation of separation of duties must happen at least annually.

Compensating Controls

Le Jardin Community Center understands that segregation of duties cannot be fully implemented in all situations. This may be due to a lack of trained personnel, job expertise, or operational functional restrictions. The following is a partial list of compensating controls that may be used in situations in which it is not possible or practical to implement segregation of duties:

- Dual Control - A process, even if not segregated fully, can still require the action of two or more individuals on a specific function.
- Job Rotation - A periodic change in job responsibilities, tasks, or the environment where work is performed allows other individuals to perform jobs and review processes or tasks that may have been performed inappropriately or have suspect activities.
- Exception Approval and Reporting - Exceptions to operations should have formalized processes to be reviewed and approved where a single individual's actions can be reviewed that are outside approved processes.
- Supervisory/Independent Activity Review - Management reviews and monitoring may detect errors or irregularities due to lack of segregation of duties.

PHYSICAL AND ENVIRONMENTAL SECURITY POLICY

OVERVIEW

Le Jardin Community Center realizes that the confidentiality, integrity, and availability of information and assets can be damaged by physical and environmental means. Le Jardin Community Center must implement appropriate controls to protect against physical and environmental threats. Physical and environmental threats include harm by malicious or unauthorized people and damage from contaminants.

SERVER ROOM

Heating/Cooling

Computer systems and networking equipment must operate within a temperature range that enables reliable operation and the longest possible life of technical components. The widest range acceptable is between 10°C/50°F and 28°C /82°F. The optimal temperature should be 20-21°C/68-71°F. The server room temperature must be monitored at all times, including nights and weekends. A systems management application which automatically monitors and alerts personnel to abnormal temperature fluctuations may be useful.

Smoke Detectors

Smoke detectors must be installed in the server room. The detector should be connected and powered within the room to enable personnel in the server room and outside the server room to detect a smoke emergency. A photoelectric smoke detector with a pulsed infrared LED light source and a high-speed photodiode sensing element are recommended in the server room.

Fire Suppression

An electronics-safe fire extinguisher must be prominently located inside the server room. All detection and monitoring devices must be tested on a regular basis as recommended by the manufacturer. Fire suppression devices must be tested for compliance with state fire marshal requirements. The date of the last test must be documented, preferably on the suppression device. Cleaning supplies must not be stored in the server room due to chemical components. There must be no smoking in the server room at any time.

Uninterruptible Power Supply (Ups)

An uninterruptible power supply must be in place and be of sufficient capacity to enable a normal shutdown in the event of power failure. If possible, UPS devices should be configured to allow a remote shutdown of servers and critical equipment as the UPS nears the end of its battery life. At a minimum the organization should plan to test UPS devices as part of an annual maintenance schedule to ensure battery life is maintained and maximum uptime is kept.

Locks/Access

Server rack must be locked at all times. Locking mechanisms should include using a multi-factor access control system. Access to the server rack may include restrictions by key. If a key system is in place, all keys must be stamped with “Do Not Duplicate.” Access rights to the server rack must be provided on a strict “need to have” basis.

All individuals accessing the server rack must sign in and out using a Server Rack Access Log. Sign-in/out includes all visitors who must be accompanied by a member of the IT staff at all times. Access log sheets must be retained by the Information Technology Department and reviewed on a periodic basis. Visitor access is restricted to departmental staff, vendors, or service personnel who are listed on an approved "Server Room Access List." Procedures regarding access requests, viewing, or touring the server room are provided below.

- Card Access - Individuals with card access to the server room are responsible for ensuring the area remains secure upon their entering or exiting. This includes deactivating and activating server room alarms.

- Visitor Access - Individuals on the "Server Rack Access List" must only have monitored, supervised access to the server room. For each access, the individual monitoring the visitor is required to record the following in the server room log book: date, visitor name, monitor name, Visitor Company or department, reason for entry, in time, and out time. All visitors must remain under IT surveillance while inside the server room and should never be left alone.

- Access Requests - Anyone without card or visitor access must request escorted access prior to being permitted to enter the server room. If the access request is approved, the visitor must follow the visitor access procedure and must be escorted at all times by personnel that have card access rights.

Wiring/Cabling

Wiring must be routed in server room away from personnel working areas and in a manner that allows for wiring and cable identification and maintenance. All wiring and cables should be properly labeled and documented to allow for easy access in the event of an issue.

Flooring

The server room floor should be above the ground level of the building. The floor must remain clear of unused wires and cables. Wires and cables must be properly protected from heat and environmental elements if on the floor.

SOCIAL MEDIA POLICY

OVERVIEW

Purpose and Scope

Le Jardin Community Center has determined that social media is a tool that can be used to further our mission and goals. Social media can provide a cost-effective method of engaging our communities in discussion, foster positive relationships with our clients, and represent Le Jardin Community Center in these emerging electronic communications.

These guidelines apply to employees, volunteers, or contractors who create or contribute to blogs, wikis, social networks, virtual worlds, or any other kind of social media and identify themselves as employees of Le Jardin Community Center or comment on the organization.

While all Le Jardin Community Center employees are welcome to participate in social media, we expect everyone who participates in online commentary to understand and to follow these simple but important guidelines. The goal is to participate online in a respectful, relevant way that protects our reputation and follows the letter and spirit of the law.

Relevant Technologies

This policy includes, but is not limited to following specific technologies:

- Twitter®
- Facebook®
- Instagram®
- Snapchat®
- Google+®
- Personal Web sites

PROCEDURES

1. Keep your work-related and personal social media accounts separate. Do not post work–related information through your personal account, or the reverse.

2. Be transparent and state that you work at Le Jardin Community Center. Your honesty will be noted in the social media environment. If you are writing about (Le Jardin Community Center), use your real name, identify that you work for Le Jardin Community Center, and be clear about your role. If you have a vested interest in what you are discussing, be the first to say so.

3. Never represent yourself or Le Jardin Community Center in a false or misleading way. All statements must be true, accurate, and not misleading; all claims must be substantiated.

4. Post meaningful, respectful comments—no spam and no remarks that are off-topic or offensive. Use common sense and common courtesy in all communication.

5. Protect sensitive or personal information. Make sure your efforts to be transparent don't violate Le Jardin Community Center's privacy, confidentiality, and legal guidelines for external communication. Never discuss clients, parents or employees of Le Jardin Community Center.

6. Limit your comments to your area of expertise and feel free to provide unique, individual perspectives on non-confidential activities at Le Jardin Community Center.

7. If you find yourself disagreeing with others' opinions, keep your response appropriate and polite. If you find yourself in a situation online that looks as if it's becoming antagonistic, do not get overly defensive and do not disengage from the conversation abruptly. Feel free to ask the HR Director for advice and/or to disengage from the dialogue in a polite manner that reflects well on Le Jardin Community Center.

8. Never comment on anything related to legal matters, litigation, or any parties Le Jardin Community Center may be in litigation with.

9. Never participate in social media when the topic being discussed may be considered a crisis situation. Even anonymous comments may be traced back to your or Le Jardin Community Center's IP address. Refer all social media activity around crisis topics to your Manager and/or the HR Director.

10. Always protect yourself, your privacy, and Le Jardin Community Center's confidential information. What you publish is widely accessible and will be around for a long time, so consider the content carefully. Social media users should always be aware that these types of communications are considered public records.
11. Personal use of social media is the right of every employee using their own equipment and on their own time. They are expected to never post or create anything that would be potentially embarrassing to Le Jardin Community Center or considered offensive. It should be clear that the views expressed are not necessarily those of Le Jardin Community Center.

DISCIPLINE FOR NONCOMPLIANCE

Personnel should be aware of potential penalties for noncompliance with organization policy, which may include suspension of certain security privileges, suspension of employment, or termination. Issues with adherence to this policy will be addressed utilizing the organization's approach to disciplinary action and with the assistance of the Human Resources Director.

SYSTEMS AND APPLICATIONS MANAGEMENT POLICY

OWNERS/CUSTODIANS/USERS

Critical assets include systems and applications that contain confidential information or have been designated as critical or highly valuable to Le Jardin Community Center. System or application criticality indicates a sense of importance or high damage level if compromised. Custodians must perform duties in collaboration with owners to protect Le Jardin Community Center assets. Users must follow owner, custodian, and Le Jardin Community Center policies and requirements.

Owner

Information owners are responsible for ensuring that information is secured according to the requirements of the information security program. Owners are responsible for reviewing access to that information to ensure access rights are appropriate. Owner's system and application requirements include:

- Responsibility for keeping an accurate inventory and location of any file, database, or other technology used to store critical information.
- The obligation to follow data retention requirements and purge data from any system so it is not retained longer than the stated retention schedule.
- Assigning classification values to information for which they have responsibility, based on its sensitivity to disclosure and for protecting it in accordance with its criticality and value.
- Ensuring that those with access to the information understand their responsibilities for collecting, using, retaining, and disposing of the information in appropriate and approved methods.
- Reviewing contractual agreements for their systems and applications to make sure they effectively provide for the protection of organization assets.

Custodian

Custodians, such as Information Technology Department personnel, are responsible for the day-to-day maintenance of information systems or information applications. Custodians are responsible to the owner of the system for ensuring proper implementation of security controls. Custodian requirements for systems and applications include:

- Establishing written procedures regarding technical implementation of granting and revoking system access privileges. Access controls are a key information technology control area.
- Monitoring system and information.

- Implementing technical policy requirements so that systems and applications are in compliance with all applicable information security policies.
- Reviewing security features installed on Le Jardin Community Center assets. This includes a review of operating systems and systems software, databases, applications, computer hardware, firewalls, security detection software, and communications hardware and software.

Users

Users Le Jardin Community systems and applications have a duty to understand the fundamental importance of information assets and recognize their responsibility for the safekeeping of those assets. Users must protect systems and applications against abuses that disrupt or threaten their security and functionality. Each user is responsible for their actions on systems and for compliance with policies concerning security and acceptable use of systems, applications, and other Le Jardin Community assets. User requirements include:

- Responsibility for their own actions to not put systems or applications at risk by inappropriate actions or negligent behavior.
- Performing information security duties as required by standards and practices.
- Restricting the use of systems and applications only to authorized individuals for authorized purposes.
- Respecting the owners and custodians' requirements for handling and protecting information.

ORGANIZATION FUNCTION

Applications must only be used for authorized Le Jardin Community purposes. All personnel must only use systems and applications that have been approved by Le Jardin Community. Users may not download or place any unapproved application, system, or software on any computer or system owned by Le Jardin Community. Personnel that desire to use a new or unapproved application must submit an application to the Information Technology Department for review and approval. Formal Organization approval must happen prior to using the new application, system, or software on any device connected to the organizational network.

APPLICATION ATTRIBUTES IMPACTING NETWORK PERFORMANCE

Service attributes of systems and applications including performance, availability, reliability, and supportability are important to Le Jardin Community. These attributes are not only measured internally but may be viewed externally by clients or vendors. The following are general practices for applications that should be reviewed to understand the performance implications of any system or application on Le Jardin Community's network.

Availability

Availability requirements for the organizational process must be defined, including:

- System uptime requirements.
- Planned periods of downtime for changes and upgrades.
- Business continuity or failure requirements.

Deployment

The information technology department needs to understand the impact of the application on Le Jardin Community's bandwidth and if usage will create disruptions in service or impact other Le Jardin Community applications' performance.

Operational Workload

Workload, such as number of business transactions processed, determines operational effectiveness of an application. Workload issues that may impact Le Jardin Community Center that should be evaluated include:

- Different usage periods at different times of the day.
- Growth projections for application use over a two-year period.
- Total number of users of the application.
- Response time expectations for application users.

Integration

Le Jardin Community Center must understand how the application integrates with other applications, systems, and business functions. If the application is a key centerpiece of the infrastructure or organizational process, extra attention will be required to examine and make sure the application can successfully integrate into the technical, business, and strategic plans of Le Jardin Community Center.

SECURE SYSTEMS DEVELOPMENT POLICY

OVERVIEW

This policy provides the requirements for secure system development and the assessment of risk during systems development. The policy applies to all systems and applications sponsored by, developed for, and maintained or operated on behalf of Le Jardin Community Center, whether the systems are operated on-site or at a non- Le Jardin Community Center location.

SPONSOR/OWNER REQUIREMENTS

Sponsor

A system development sponsor is an individual or department that has requested, procured, funded, or authorized the development or enhancement to a system. System development sponsors are responsible for providing adequate business requirements for the development of the system. Sponsors must provide adequate department resources to assist in the development of the systems.

Owner

The system owner is the individual or department responsible for daily operations of a system, including maintenance. The owner is responsible for ensuring secure system standards are followed for their assigned system(s).

Development Scope.

Methodology

The Information Technology Committee is responsible for approving final security requirements for systems. It is the responsibility of the Information Technology Committee to document acceptance of the security requirements by sponsors and owners for each new system or system acquisition. The Information Technology Committee should also review and accept system tests against the security requirements. The Committee must approve a development methodology that includes security controls. It is recommended that systems be designed with security requirements integrated into the original design rather than making subsequent changes after implementation.

Le Jardin Community Center's system development activities must incorporate appropriate security controls and activity logs. System security controls must include validation controls for

any data entry and data processing. Data entry validation controls include access controls including:

- Controls over entry and changes to data.
- Error checks.
- Review of suspicious or unusual data.
- Appropriate review and authorization for highly sensitive transactions or data.

Some Le Jardin Community Center systems may require the integration of additional authentication and encryption controls to ensure integrity and confidentiality of the data. Ongoing risk assessments must be performed by Le Jardin Community Center to consider the adequacy of system level controls in light of changing threat environments.

Project Plan

The project plan must include system security requirements as part of the development process within Le Jardin Community Center's software development methodology. The depth and detail of the project plan provide an indicator of system and security maturity within Le Jardin Community Center.

Project plan security requirements may include:

- Establishment of security classification levels of systems and data.
- Clarification of departmental functional security requirements and acceptance criteria.
- Use of secure coding standards.
- Tests and reviews for compliance with security requirements, code development, and testing processes.
- Requirements from nondisclosure agreements to protect Le Jardin Community Center's rights to source code and customer data as appropriate.
- Requirements from completed service level agreements that dictate security requirements relating to system performance and emergency response.
- Restrictions on developer write access to production source code and systems
- Monitoring of inappropriate access to development systems.
- Physical security over developer work areas, including restrictions on Le Jardin Community Center assets or information taken to and from the work area.

Security Requirements

- Each system must have a system owner designated for each system that is developed, purchased, operated, or maintained by their respective departments.
- Le Jardin Community Center must implement secure development procedures during the following:

- New system development projects must create security requirements during the “Requirements” phase of the development lifecycle.
- All systems containing critical or confidential data or systems that are integrated with systems containing critical or confidential data must be reviewed for appropriate security requirements at least every two years.
- All systems must be reviewed for appropriate security requirements when any significant changes are planned for the system.

- A risk assessment will be performed prior to the production implementation of all Commercial-off-the-shelf (COTS) systems purchased, operated, or maintained by Le Jardin Community Center.

TESTING AND QUALITY

The following list contains items that may be used to review and/or test security within the development process:

- Security requirements in the project scope and budget.
- Classification of information within the system or application.
- Risk assessment completion.
- Separation of duties review.
- Design and network diagram documentation that includes security components.
- Data sharing requirements.
- Data handling requirements.
- Software licensing and registration requirements.
- Inventory of hardware and software assets impacted by the system.
- Remote access controls.
- Authorization based on least privilege and need to know.
- Authentication requirements.
- Malware or malicious code review.
- Auditing and logging controls.
- Information transmission requirements.
- Backup requirements.
- Business continuity and disaster recovery plan for system.
- Security integration with:

    - Software project files.
    - Unit, system integration and acceptance test plans.
    - Operational documentation.
    - Training.
    - Business acceptance testing.

- Change management.

IMPLEMENTATION

Systems development processes should include a sign-off by system owners that a security review has taken place and that any department security requirements have been met. This review must take place prior to production implementation.

SUPPORT AND MAINTENANCE

Project plans will describe how ongoing security reviews will take place to show appropriate Le Jardin Community Center support and maintenance for the system after initial implementation. Ongoing system reviews must include additional or changed security requirements that Le Jardin Community Center has adopted since the original development plan.

TECHNOLOGY COMMITTEE POLICY OR CHARTER

OVERVIEW

The Technology Committee's (Committee) goal is to improve the effectiveness in the use and management of information technology at Le Jardin Community Center. Managing information technology through the Committee will be accomplished through monitoring, evaluating, and overseeing the implementation of policies and solutions to maintain or enhance technology functions. The Committee will also assist Le Jardin Community Center management in making informed technological decisions without requiring them to become involved in daily or routine information technology operations. Committees also serve as advocates for the Information Technology Department and effective communication channels in regard to the decision-making process. The members are able to explain how and why a particular decision was made.

Scope

The Committee will perform the duties listed below in addition to any other duties the executive management of Le Jardin Community Center might assign to the Committee. Executive management must be provided with Committee minutes after each Committee meeting. Committee members may immediately report to executive management or department heads any issues that require specific or immediate attention, such as any significant issues with major technology initiatives or information security breaches.

Membership

Committee membership must include employees with knowledge of Le Jardin Community Center information technology and operations. Also, all core functional areas of Le Jardin Community Center should be represented on the Committee. A broad-based membership will ensure that the Committee meetings and actions out of the Committee will work in tandem with departmental requirements and expectations. Additions or changes to Committee membership will be determined by the Committee Chairperson and the Executive Director. The Committee Chairperson may be the Information Technology Specialist or Le Jardin Community Center may select another Chairperson from the Executive Management team to oversee each meeting and be responsible for final Committee decisions.

Program Oversight

The Committee is accountable to executive management and will be provided the right of obtaining any information regarding Le Jardin Community Center technology assets. Necessary information may include information from the Information Technology Department, end-user or operational departments. In addition, the Committee may request authorized expenditures with executive management approval to implement strategies and procedures to resolve technical

problems or enhance confidentiality, integrity, or availability of Le Jardin Community Center computer systems.

TECHNOLOGY MANAGEMENT

The Committee shall perform the following duties:

Technology Governance and Board Updates

- Create and maintain an Information Technology Strategic Plan aligned with organization-wide initiatives, often spanning a one- to three-year time frame.
- Oversee information technology budgeting decisions, providing oversight regarding resources and risk assessment.
- Oversee the updating, reviewing and approving of Information Technology policies.
- Review and create mitigation plans to address regulatory issues involving technology and technology audit findings and determine scope and frequency for external testing of information technology and information security.
- Annually present to executive management a formal overview of the information technology and information security activities. The overview will address updates to policies, technology and information security risk assessments and risk posture, Committee recommendations, regulatory compliance, disaster recovery plans and testing, vendor risk analysis, the overall status of the program, and any other important components dealing with information technology or information security.
- Present the executive management team with timely updates on security breaches, changes to Le Jardin Community Center risk profile, major information technology project changes or information technology initiatives, and any other issue deemed appropriate by the Committee.

Vendor Management

- Ensure the qualifications of vendors used to provide information technology services through an annual review process.
- Update and review Le Jardin Community Center vendor management procedures.

Information Security

- Maintain, test, and train employees on the information security program and individual information security responsibilities.
- Provide ongoing information security awareness training on prevalent topics to all employees.
- Maintain current information technology infrastructure reviews and information security risk assessments, and use them to determine appropriate resource and asset use within the organization.

Systems (Network and Applications)

- Ensure adequate controls and change management procedures are in place to protect the organization's network and applications.
- Review internal problem reports and change management logs to detect major changes or problems.
- Address system functionality to meet ongoing and future Le Jardin Community Center requirements.

MEETING PLANNING

Committee meetings will be conducted quarterly, and discussion topics will be determined by the chairperson based on prior events, regulatory or Le Jardin Community Center changes, and the Technology Committee Schedule. However, the Committee may need to meet more frequently based on adapting to changing risks, regulations, and technology. Priority at meetings will be given to critical enterprise strategic initiatives or emergency/incident response issues as needed.

Meeting minutes will be documented by an appointed Committee secretary and will be presented for review to executive management within two days following a Committee meeting. In addition to Committee minutes, an Issue Tracking Form will be utilized at each meeting to track issues and projects through completion. Committee meeting minutes and records will be retained for five years and will be made available to the executive management and Committee members.

TRAINING POLICY

OVERVIEW

Personnel training is an important part of the information technology and information security program. Proper training reduces time Le Jardin Community Center needs to spend on incidents, public relations, notification, and information recovery. Technical controls alone do not fully protect Le Jardin Community Center. Human error or intentional malfeasance can be the most dangerous threat facing Le Jardin Community Center. Security awareness and training helps to ensure that all individuals who handle Le Jardin Community Center's assets will be aware of their responsibility to protect the organization's information and systems. All personnel must successfully complete training so that they understand their roles and responsibilities regarding information assets and are able to comply with information security policies.

TRAINING REQUIREMENTS

Information Security Training

Information security training will be provided to all personnel authorized to access Le Jardin Community Center systems, including employees, vendors, and contractors. New personnel are required to successfully complete information security training within the first 90 days of employment and annually affirm their understanding of and intent to comply with the information security policy. Training and affirmation for all personnel must be completed annually. The IT Specialist in collaboration with department managers, must provide ongoing information security awareness to personnel.

Technology Training

Technical training must be provided for all systems personnel. Training may include mentoring by senior employees, online courses, offsite courses, or reading technical books, magazines, and manuals. It is expected that all systems personnel will be competent to perform their assigned job function and will continually strive to gain additional technical knowledge to assist Le Jardin Community Center.

Regulatory Training

Certain Le Jardin Community Center personnel may have the need for training on specific regulatory, government, or agency rules or functions. This may include federal, state, and local regulations and requirements. Personnel that have these additional knowledge requirements should be trained to effectively represent the organization.

TRAINING SCHEDULE

Security Training

All employees of Le Jardin Community Center must take part in ongoing training provided on information security and technology provided on a monthly basis. Training may be provided in a web-based format, on a one-on-one basis or in a group setting, as deemed appropriate by Le Jardin Community Center. Employees will be required to schedule time to participate in these training sessions, and tracking must be performed to ensure all personnel has completed the necessary training. Training may be performed by individuals from Information Technology, Information Security, or by outside consultants as necessary.

Additional Training Requests

If Le Jardin Community Center personnel require additional training to perform their job function, a request may be sent to their manager. The manager and relevant department leaders or executive management will determine the appropriate action necessary to provide the training requested. Although Le Jardin Community Center supports furthering the education of personnel, not all requests for additional training may be accepted. Upon approval, the employee will work with their manager to determine the appropriate source for providing the training.

PROGRAM MANAGEMENT RESPONSIBILITY

Information security training will be the responsibility of the IT Specialist, as deemed appropriate by Le Jardin Community Center. Regulatory training will be the responsibility of the senior management of the department with the regulatory training requirements.

All the individuals responsible for creating and managing training shall perform the following:

- Provide input into the security awareness and training program.
- Identify training requirements based on needs of Le Jardin Community Center and risks to Le Jardin Community Center's business.
- Develop an annual training program strategy and plan.
- Budget for training and awareness activities.
- Coordinate all training program activities.

Preparation and application of training

VENDOR MANAGEMENT POLICY

OVERVIEW

Le Jardin Community Center utilizes services from external suppliers, service providers, software companies, and other consultants and vendors. This policy uses the term 'vendor' to cover all non-employee organizations or individuals that provide services to Le Jardin Community Center. These services may include vendors that have contact Le Jardin Community Center's confidential information, transaction processing services, or other activities. The use of these external vendors may expose the organization to regulatory, financial, or organizational reputation risk. While properly defined vendor contracts address some risk factors, Le Jardin Community Center continues to be responsible for certain additional risks. In order to mitigate these risks, Le Jardin Community Center must verify the ability of existing vendors to manage risks which may be passed on to Le Jardin Community Center and manage contracts with vendors.

Le Jardin Community Center will update a comprehensive list of vendors annually and must analyze each vendor based on the nature of the services or products provided and their importance to the organization. Vendors will be assigned a risk rating, with critical vendors receiving additional validation and review. In addition, Le Jardin Community Center must perform certain due diligence analysis prior to engaging any new or additional vendors.

VENDOR CLASSIFICATION

The Technology Committee and IT Specialist must evaluate vendors to ensure that appropriate performance standards have been outlined in the contract. The Le Jardin Community Center must also perform monitoring of the vendor for performance against contractual and service level requirements. The Technology Committee and IT Specialist will review the list of current vendors and prepare an annual assessment of criticality for each vendor or service provider. The following factors must be considered:

- Potential impact on Le Jardin Community Center's ability to deliver minimum levels of service to clients, and the impact of not providing the services in question.
- Potential losses to Le Jardin Community Center in relation to the provided service.
- Le Jardin Community Center's ability to meet regulatory and/or funder requirements, and to control or monitor the vendor's compliance with regulatory and/or funder requirements.
-

The following tables show risk ratings and descriptions of High, Medium, and Low vendor criticality. When a vendor has risk rating values of different levels across several categories, the value for each vendor that ranks highest in criticality will determine the overall criticality rating for that vendor.

Vendor Criticality Risk Rating

Critical Vendors - (High Rating)	
SERVICES	Required for adequate service delivery capabilities or to maintain acceptable customer service levels
RISK LEVELS	Vendor exposes Le Jardin Community Center to significant fiscal, operational, or reputation risks
VENDOR HEALTH	There is a significant amount of financial risk to the vendor company
INFORMATION	Vendor has significant access to confidential or customer information for Le Jardin Community Center.
REPLACEMENT	There is no immediate replacement or back-up for services provided, or they could be the only source of the service for a single or several locations
LOSS EXPOSURE	Vendor's failure to adequately manage risk could result in significant losses
Important Vendors - (Medium Rating)	
SERVICES	Le Jardin Community Center could maintain minimum operational capability without the vendor's service
RISK LEVELS	Moderate operational risk, but Le Jardin Community Center has controls and monitoring in place to mitigate risks to operations
VENDOR HEALTH	Vendor company and industry are subject to moderate credit or financial risk due to the nature of the service or products provided
INFORMATION	Systematic, limited confidential information available to vendor; controls in place
REPLACEMENT	There are replacement vendors or back-ups available to ensure service continuity
LOSS EXPOSURE	Acceptable losses may be incurred should vendor fail to adequately manage risk
Incidental Vendors - (Low Rating)	
SERVICES	Service delivery capability or operational levels would not be immediately impacted by loss or replacement of vendor
RISK LEVELS	Minimal risk to Le Jardin Community Center, or Le Jardin Community Center has significant control over potential risk
VENDOR HEALTH	Vendor company is exposed to negligible financial risk
INFORMATION	Vendor has only incidental contact with confidential information
REPLACEMENT	Acceptable alternatives are available for use with little or no financial impact
LOSS EXPOSURE	Minimal or no losses would result from vendor failure to adequately manage risk

VENDOR SELECTION AND CONTRACTING

Prior to signing a contract with any critical vendors, Le Jardin Community Center must assess the risks from the services provided by the vendor. The organization must also evaluate controls for mitigating these risks. It is the responsibility of the manager acquiring the service to evaluate the related vendor risk using the criteria provided. This can be done by completing a Vendor Relationship Risk Assessment (located in the templates provided with this policy) and submitting it to the Technology Committee to ensure that an appropriate evaluation has been made.

The risk assessment must include the evaluation of the following factors:

- The criticality of the function to Le Jardin Community Center.
- Information security controls of the vendor (may be reviewed in Service Organization Control (SOC) reports or other reports prepared by external parties, such as consulting or audit firms).
- The nature of services to be performed by the vendor.
- The availability of alternative vendors for the particular function.
- Insurance coverage available for particular risks.
- The cost and time required to change vendors if issues arise.
- A determination that Le Jardin Community Center understands the roles, responsibilities, and contractual obligations of all parties.

New Vendor Relationship Process

1. **Vendor Selection and Risk Assessment** - In addition Le Jardin Community Center purchasing requirements, the organization must prepare a Vendor Relationship Risk Assessment and perform a review and due diligence of the vendor. Le Jardin Community Center must be confident regarding the vendor's competence and stability, both financially and operationally, to provide the contractual services and meet any related commitments. This activity provides an opportunity to reduce the risk that a vendor will surprise the organization in failing to provide critical services in the coming year. In some cases vendor financial statements, preferably audited statements, may be obtained and reviewed by the Technology Committee or their designee.
2. **Contract Approval** - Terms and conditions of each contract will be reviewed by Le Jardin Community Center to ensure that they are appropriate for the particular service being provided and result in an acceptable level of risk. In some cases, the organization may have the contract reviewed by their legal counsel as well, based on the overall risk rating for the vendor. The written contract between Le Jardin Community Center and the vendor should clearly specify, at a level of detail appropriate to the scope and risks of the service to be provided, all relevant terms, conditions, responsibilities, and liabilities of both parties. These would normally include:

- Agreements not to disclose non-public information either in possession of the vendor or accessible to them and statements of responsibility and liability for disclosure of such information.
- Statements of the purpose of access to or maintenance of any non-public information.
- Required service levels, performance standards, and penalties. This is often referred to as the Service Level Agreement (SLA) component.
- Compliance with applicable regulatory requirements.
- Internal controls, insurance, disaster recovery capabilities, and other risk management measures maintained by the vendor.
- Provisions for access to internal/external audits or other reviews of the vendor's operations and financial condition.
- Data and system ownership and access.
- Applicable insurance coverage.
- Liability for delayed or erroneous transactions and other potential risks.
- Provisions for handling disputes, contract changes, and contract termination.

3. **Establishment and Approval of Controls** – If the vendor will have offsite access or the ability to view or change Le Jardin Community Center confidential information outside of the protected Le Jardin Community Center network, the vendor must implement appropriate internal control policies and procedures, data security and disaster recovery capabilities, and other operational controls in line with those that Le Jardin Community Center would utilize if the activity were performed internally. If the vendor will only have controlled access onsite or only viewing of information over Le Jardin Community Center network, the vendor must agree to follow all Le Jardin Community Center policies while performing Le Jardin Community Center services. In the case of critical vendors, the organization may ask to review vendor's policies and procedures.
4. **Ongoing Monitoring** - Le Jardin Community Center must review the operational performance of vendors on an annual basis. The Technology Committee or their designee will be responsible for completing this evaluation. In addition, Le Jardin Community Center must update contact information for all vendors, regardless of their criticality rating, at least annually.
5. **Information Access** - Le Jardin Community Center must ensure that it has complete and immediate access to current and appropriate back-up information. This can include testing disaster recovery and backup data access, as well as reviewing the results of vendor testing.
6. **Contingency Plans** - Le Jardin Community Center must ensure that appropriate business continuity and disaster recovery plans have been prepared and tested by critical vendors.
7. **Notification of Regulators** - Service provider change notification must be provided to any regulatory agencies as required.

ONGOING VENDOR RISK EVALUATIONS:

As mentioned previously, Le Jardin Community Center will evaluate the risks and exposures associated with all vendor relationships annually. This evaluation process will include the following:

- Updating all vendor listings and contact information.
- Updating vendor information for Incident Response and Disaster Recovery policies.
- Determining and assigning risk ratings to each vendor using Le Jardin Community Center vendor criticality ratings.
- Completing Vendor Risk Assessments for critical vendors.
- Completing a Vendor Information Safeguard Review for critical vendors.
- Reporting any notable changes or findings to the Technology Committee or management in a timely manner.

CORPORATE AND PERSONALLY OWNED MOBILE DEVICE POLICY

OVERVIEW

The increase of both personally owned and organization owned mobile devices has drastically increased. Mobile devices can assist in user productivity but also expose the organization to security risks. The Le Jardin Community Center will establish the criteria governing the authorized use of personal or organization owned mobile devices (device), including (but not limited to) smart phones, iPads, notebooks, tablet PCs and tablet PCs that perform similar functions as laptops but may not have all the protections as a laptop. The policy differentiates policy requirements based on ownership of the device, use of the device, and whether organization data will be stored on the device. The goal of the policy is to allow the users of Le Jardin Community Center the privilege to use a mobile device while also protecting the confidential data of the organization.

POLICY

General

Le Jardin Community Center allows its users the privilege of using mobile devices, for certain organization functions, but only with prior approval from the organization Le Jardin Community Center will grant device access to email, applications, systems, or other organization assets on a case-by-case basis. The Information Technology department controls which types (brands and models) and versions of smartphones or tablets will be allowed access to any organization asset, including email, applications, systems, or data. Other Le Jardin Community Center policies, including but not limited to Acceptable Use and Social Media, will also apply to the use of the device. Le Jardin Community Center reserves the right to revoke this privilege if users do not abide by the policies and procedures outlined below Le Jardin Community Center reserves the right to take appropriate disciplinary action up to and including termination for noncompliance with this policy.

Enrollment

In order to enroll your device, the device must be registered with the Le Jardin Community Center. To register, complete a Mobile Device Request Form. This form is used for both requests for purchasing organization owned devices and for personally owned devices access to email, applications, systems, or other organization assets. Generally, personally owned devices will only be allowed access to the organization's email server and will not be allowed to connect to the network. The concept of allowing personally owned devices to access Organizational resources is termed bring your own device (BYOD). Organization owned devices will be provided with access to applications or systems based on need.

Requirements for All Devices

The following requirements are in place for all users of approved devices:

- The user is responsible for the installation of device software updates during the use of the device.
- Users must report lost or stolen device immediately (within 24 hours).
- The devices' camera and/or video capabilities may not be used while on organization premises during the class on the children.
- Users may not store or transmit illicit materials.
- Users may not store or transmit proprietary information belonging to another organization on the device.
- Devices must be password protected using the strongest features of the device.
- Strong passwords are required to access the organization network.
- The device must lock itself with a password or PIN if it's idle for five minutes.
- If the user has access to confidential data or stores organization data on the device (excluding email), the device must be encrypted.
- The user is responsible for securing their device to prevent confidential data from being lost or compromised and to prevent viruses from being spread.
- Users are forbidden from copying confidential data from email, calendar and contact applications to other applications on the device or to an unregistered/unenrolled personally owned device.
- If storage of organization data is approved on the device, the device must be configured to segregate organization data from personal data.

Organization Owned Devices

The following requirements are in place for all users of organization owned devices:

- There is a zero-tolerance policy for texting or emailing while driving with the device and only hands-free talking while driving is permitted (based on state laws).
- After five failed login attempts, the device will lock. Information Technology must be contacted to regain access.
- Rooted (Android) or jailbroken (iOS) devices are strictly forbidden from accessing the organization's network.
- Users may not download, install or use any app that does not appear on the organization's list of approved apps.
- The device may be remotely wiped, disconnected or disabled at any time. The most common uses of remote wipe will be if the device is lost, the user terminates his or her employment or is terminated from employment, or Information Technology detects a data or policy breach, a virus or similar threat to the security of the organization's data and technology infrastructure.
- The Organization has the right to at will monitor organization messaging systems and data including data residing on the user's device.
- Removal of device security controls is prohibited.

- Random spot checks of the device configuration may occur to ensure compliance with all applicable security policies.
- All wireless LAN access provisioned to the organization' network must use organization-approved vendor products and security configurations.

Personally Owned Devices

The following requirements are in place for all users of organization owned devices:

- The user is personally liable for all costs associated with his or her device.
- The user assumes full liability for risks including, but not limited to, the partial or complete loss of organization and personal data due to an operating system crash, errors, bugs, viruses, malware, and/or other software or hardware failures, or programming errors that render the device unusable.
- The user is responsible for keeping his or her device in their possession or properly securing it, at all times. The organization is not responsible for the security or condition of user's personal devices.
- The user is responsible for the proper care of personal technology devices, including all maintenance and repair, replacement or modifications, and software updates necessary to effectively use the device.
- Personal devices may not be plugged into the organization's wired network without approval from the Information Technology department.
- If the user is allowed to store organization data on the device, the Information Technology department will be allowed to perform security precautions, such as a remote wipe, based on incident. Users must take responsibility to consistently back up any personal data in the event of a remote wipe by the organization.
- Personally owned devices (in accordance with the BYOD – bring your own device - concept) may only access Organization resources, such as email and calendar functions, after receiving approval from the Information Technology Specialist and their first line manager.

Organization Information Technology Responsibilities

Information Technology Personnel Responsibility for Organization Owned Devices:

- Enabling the device to access the web-based interface of the email system.
- Email, Calendar and Contact Sync service configuration.
- Wi-Fi Internet Access configuration.
- Unsubscribing devices not compliant with secure configuration standards.
- Device reset and data deletion.
- Device encryption options.
- Installation of a Mobile Device Management solution on the device
- Devices configuration of standard apps, such as browsers, office productivity software and security tools of the device.