LAKEMARY
CENTER

Employee General Technology Standards

Lakemary Employee General Technology Standards
Originated: Prior to 2016
Reviewed:
Revised: 01/16; 05/18; 07/20; 10/20; 08/21; 09/23; 9/24

Lakemary, Inc.

1 Introduction

Lakemary (LMC) provides computers, peripherals, email accounts, internet access (wired or wireless) and server file access (collectively referred to as computer systems) as needed for employees to perform their stated duties. The computer systems are the property of LMC and may be accessed, monitored, altered or removed from operation at the discretion of LMC management. These guidelines set forth LMC’s standards and procedures for the access and use of computer systems. Violation of these standards may result in appropriate disciplinary action up to and including discharge.

LMC management and the Information Technology (IT) Department’s intentions for publishing Technology Standards and Procedures are not to impose rigid restrictions that are contrary to Lakemary’s established culture of openness, trust and integrity. LMC management and the IT Department are committed to protecting Lakemary's employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

2 Acceptable Use Standard

2.1 Overview

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of Lakemary. These systems are to be used for business purposes in serving the interests of the company, and of our clients and customers in the course of normal operations.

Effective security is a team effort involving the participation and support of every Lakemary employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

2.2 Purpose

The purpose of this Standard is to outline the acceptable use of computer equipment at Lakemary. These rules are in place to protect the employee and Lakemary. Inappropriate use exposes Lakemary to risks including virus attacks, compromise of network systems and services, and legal issues.

2.3 Scope

This Standard applies to the use of information, electronic and computing devices, and network resources to conduct Lakemary business or interact with internal networks and business systems, whether owned or leased by Lakemary, the employee, or a third party. All employees, contractors, consultants, temporary, and other workers at Lakemary and its subsidiaries are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with Lakemary policies and standards, and local laws and regulation.

This Standard applies to employees, contractors, consultants, temporaries, and other workers at Lakemary, including all personnel affiliated with third parties. This Standard applies to all equipment that is owned or leased by Lakemary, as well as third parties accessing Lakemary network resources.

2.4 Standard

2.4.1 General Use and Ownership

2.4.1.1 Lakemary proprietary information stored on electronic and computing devices whether owned or leased by Lakemary, the employee or a third party, remains the sole property of Lakemary. You must ensure through legal or technical means that proprietary information is protected in accordance with the Data Protection Standard.

2.4.1.2 You have a responsibility to promptly report the theft, loss or unauthorized disclosure of Lakemary proprietary information.

2.4.1.3 You may access, use or share Lakemary proprietary information only to the extent it is authorized and necessary to fulfill your assigned job duties.

2.4.1.4 Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.

2.4.1.5 For security and network maintenance purposes, authorized individuals within Lakemary may monitor equipment, systems and network traffic at any time.

2.4.1.6 Lakemary reserves the right to audit networks and systems on a periodic basis to ensure compliance with this Standard.

2.4.2 Security and Proprietary Information

2.4.2.1 All mobile and computing devices that connect to the internal network must comply with the Minimum Access Standard.

2.4.2.2 System level and user level passwords must comply with the Password Construction Guidelines and Password Protection Standard. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.

2.4.2.3 All computing devices must be secured with a password-protected screensaver with the automatic activation feature set to 10 minutes or less. You must lock the screen or log off when the device is unattended.

2.4.2.4 Postings by employees from a Lakemary email address should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Lakemary, unless posting is in the course of business duties.

2.4.2.5 Employees must use extreme caution when opening e-mail attachments or clicking on links received from unknown senders, which may contain malware.

2.5 Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of Lakemary authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Lakemary-owned resources.

The lists below are by no means exhaustive but attempt to provide a framework for activities which fall into the category of unacceptable use.

2.5.1 System and Network Activities

The following activities are strictly prohibited:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Lakemary.
2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Lakemary or the end user does not have an active license is strictly prohibited.
3. Accessing data, a server or an account for any purpose other than conducting Lakemary business, even if you have authorized access, is prohibited.
4. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
5. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
6. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
7. Using a Lakemary computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
8. Making fraudulent offers of products, items, or services originating from any Lakemary account.
9. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.

10. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

11. Port scanning or security scanning is expressly prohibited unless prior notification to the IT Department is made.

12. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.

13. Circumventing user authentication or security of any host, network or account.

14. Introducing honeypots, honeynets, or similar technology on the Lakemary network (See Section 7 for Definitions and Terms).

15. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).

16. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.

17. Providing information about, or lists of, Lakemary employees or consumers/clients to parties outside Lakemary.

2.5.2 Email and Communication Activities

When using company resources to access and use the Internet, users must realize they represent the company. Whenever employees state an affiliation to the company, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of the company". Questions may be addressed to the IT Department.

The following activities are strictly prohibited (See also *Email Standard*):

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).

2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.

3. Unauthorized use, or forging, of email header information.

4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.

5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
6. Use of unsolicited email originating from within Lakemary's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by Lakemary or connected via Lakemary's network.

2.6 Standard Compliance

2.6.1 Compliance Measurement

The IT Department team will verify compliance to this Standard through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the Standard owner.

2.6.2 Exceptions

Any exception to the Standard must be approved by the IT Department team in advance.

2.6.3 Non-Compliance

An employee found to have violated this Standard may be subject to disciplinary action, up to and including termination of employment.

2.7 Related Standards and Processes

- *Data Protection Standard*
- *Minimum Access Standard*
- *Password Construction Guidelines*
- *Password Protection Standards*

2.8 Definitions and Terms

The following definition and terms can be found in the SANS Glossary located at: https://www.sans.org/security-resources/glossary-of-terms/

- Blogging
- Honeypot
- Honeynet
- Proprietary Information
- Spam

3 Password Guidelines

3.1 Overview

Passwords are a critical component of information security. Passwords serve to protect user accounts; however, a poorly constructed password may result in the compromise of individual systems, data, or the Lakemary network. This guideline provides best practices for creating secure passwords.

3.2 Purpose

The purpose of these guidelines is to provide best practices for the creation of strong passwords.

3.3 Scope

These guidelines apply to employees, contractors, consultants, temporary and other workers at Lakemary, including all personnel affiliated with third parties. These guidelines apply to all passwords including but not limited to user-level accounts, system-level accounts, web accounts, e-mail accounts, screen saver protection, voicemail, and local router logins.

3.4 Statement of Guidelines

All passwords should meet or exceed the following guidelines

Strong passwords have the following characteristics:

- Contain at least 8 alphanumeric characters.
- Contain both upper and lower case letters.
- Contain at least one number (for example, 0-9) and/or…
- Contain at least one special character (for example, ! $%^&*()_+|~-=\`{}[]:";'<>?,/).

You should never write down a password. Instead, try to create passwords that you can remember easily. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase, "This May Be One Way To Remember" could become the password TmB1w2R! or another variation.

Passwords must not be shared with anyone for any reason. All passwords are to be treated as sensitive, Confidential Lakemary information. Corporate Information Security recognizes that legacy applications do not support proxy systems in place.

4 Email Standard

4.1 Overview

Electronic email is pervasively used in almost all industry verticals and is often the primary communication and awareness method within an organization. At the same time, misuse of email can post many legal, privacy and security risks, thus, it is important for users to understand the appropriate use of electronic communications.

4.2 Purpose

The purpose of this standard is to ensure the proper use of the Lakemary email system and make users aware of what Lakemary deems as acceptable and unacceptable use of its email system. This standard outlines the minimum requirements for use of email within the Lakemary Network.

4.3 Scope

This standard covers appropriate use of any email sent from a Lakemary email address and applies to all employees, vendors, and agents operating on behalf of Lakemary.

4.4 Standard

4.4.1 All use of email must be consistent with Lakemary policies and standards of ethical conduct, safety, compliance with applicable laws and proper business practices.

4.4.2 Lakemary email account should be used primarily for Lakemary business-related purposes; personal communication is permitted on a limited basis, but non-Lakemary related commercial uses are prohibited.

4.4.3 All Lakemary data contained within an email message or an attachment must be secured according to the *Data Classification and Protection Standard*.

4.4.4 Email should be retained only if it qualifies as a Lakemary business record. Email is a Lakemary business record if there exists a legitimate and ongoing business reason to preserve the information contained in the email.

4.4.5 Email that is identified as a Lakemary business record shall be retained according to Lakemary Record Retention Schedule.

4.4.6 The Lakemary email system shall not to be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair color, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Employees who receive any emails with this content from any Lakemary employee should report the matter to their supervisor immediately.

4.4.7 Users are prohibited from automatically forwarding Lakemary email to a third party email system (noted in 4.4.8 below). Individual messages which are forwarded by the user must not contain Lakemary confidential (e.g. PHI, PII) or above information (noted in 4.4.6).

4.4.8 Users are prohibited from using third-party email systems and storage servers such as Google, Yahoo, and MSN Hotmail etc. to conduct Lakemary business, to create or memorialize any binding transactions, or to store or retain email on behalf of Lakemary. Such communications and transactions should be conducted through proper channels using Lakemary-approved documentation.

4.4.9 Using a reasonable amount of Lakemary resources for personal emails is acceptable, but non-work related email shall be saved in a separate folder from work related email. Sending chain letters or joke emails from a Lakemary email account is prohibited.

4.4.10 Lakemary employees shall have no expectation of privacy in anything they store, send or receive on the company's email system.

4.4.11 Users are prohibited, unless an exception is granted under section 5.5.2 of this standard, from accessing email outside of the Lakemary local area network (LAN).

4.4.12 Lakemary may monitor messages without prior notice.

4.4.13 Multi-Factor Authentication is required when accessing Email or Office 365 outside of Lakemary's main network

4.5 Standard Compliance

4.5.1 Compliance Measurement

The IT Department team will verify compliance to this standard through various methods, including but not limited to, periodic walk-thrus, business tool reports, internal and external audits (e.g., Office 365 logs), and feedback to the standard owner.

4.5.2 Exceptions

Any exception to the standard must be approved by the relevant department head and the IT Department in advance.

4.5.3 Non-Compliance

An employee found to have violated this standard may be subject to disciplinary action, up to and including termination of employment.

4.6 Related Standards, Policies and Processes

- Data Protection Standard

4.7 Definitions and Terms

None.

5 Workstation Security (For HIPAA) Standard

5.1 Overview

See Purpose.

5.2 Purpose

The purpose of this standard is to provide guidance for workstation security for Lakemary workstations in order to ensure the security of information on the workstation and information the workstation may have access to. Additionally, the standard provides guidance to ensure the requirements of the HIPAA Security Rule “Workstation Security” Standard 164.310(c) are met.

5.3 Scope

This standard applies to all Lakemary employees, contractors, workforce members, vendors and agents with a Lakemary-owned or personal-workstation connected to the Lakemary network.

5.4 Standard

Appropriate measures must be taken when using workstations to ensure the confidentiality, integrity and availability of sensitive information, including protected health information (PHI) and that access to sensitive information is restricted to authorized users.

5.4.1 Workforce members using workstations shall consider the sensitivity of the information, including protected health information (PHI) that may be accessed and minimize the possibility of unauthorized access.

5.4.2 Lakemary will implement physical and technical safeguards for all workstations that access electronic protected health information to restrict access to authorized users.

5.4.3 Appropriate measures include:

- Restricting physical access to workstations to only authorized personnel.
- Securing workstations (screen lock or logout) prior to leaving area to prevent unauthorized access.
- Enabling a password-protected screen saver with a short timeout period to ensure that workstations that were left unsecured will be protected. The password must comply with Lakemary *Password Construction Guidelines*.
- Complying with all applicable password policies and standards. See Lakemary *Password Construction Guidelines and Password Protection Standard*.
- Ensuring workstations are used for authorized business purposes only.
- Never installing unauthorized software on workstations.

- Storing all sensitive information, including protected health information (PHI) on network servers
- Keeping food and drink away from workstations in order to avoid accidental spills.
- Securing laptops that contain sensitive information by using cable locks or locking laptops up in drawers or cabinets.
- Complying with the *Acceptable Encryption Standard*
- Installing privacy screen filters or using other physical barriers to alleviate exposing data.
- Ensuring workstations are left on but logged off in order to facilitate after-hours updates.
- Exit running applications and close open documents
- Ensuring that all workstations use a surge protector (not just a power strip) or a UPS (battery backup).
- If wireless network access is used, ensure access is secure by following the *Wireless Infrastructure Standard*.

5.5 Standard Compliance

5.1 Compliance Measurement
The IT Department team will verify compliance to this standard through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the standard owner.

5.5.1 Exceptions

Any exception to the standard must be approved by the IT Department in advance.

5.5.2 Non-Compliance

An employee found to have violated this standard may be subject to disciplinary action, up to and including termination of employment.

5.6 Related Standards, Policies and Processes

- Password Standard
- Portable Workstation Encryption Standard
- Wireless Infrastructure Standard
- Workstation Configuration Standard
- HIPAA Privacy Standards
- HIPAA Security Standards

HIPPA 164.210
http://www.hipaasurvivalguide.com/hipaa-regulations/164-310.php

About HIPPA
http://abouthipaa.com/about-hipaa/hipaa-hitech-resources/hipaa-security-final-rule/164-308a1i-administrative-safeguards-standard-security-management-process-5-3-2-2/

5.7 Definitions and Terms

None.

6 Wireless Communication Procedure

6.1 Overview

With the mass explosion of Smart Phones and Tablets, pervasive wireless connectivity is almost a given at any organization. Insecure wireless configuration can provide an easy open door for malicious threat actors.

6.2 Purpose

The purpose of this procedure is to secure and protect the information assets owned by Lakemary. Lakemary provides computer devices, networks, and other electronic information systems to meet missions, goals, and initiatives. Lakemary grants access to these resources as a privilege and must manage them responsibly to maintain the confidentiality, integrity, and availability of all information assets.

This procedure specifies the conditions that wireless infrastructure devices must satisfy to connect to Lakemary network. Only those wireless infrastructure devices that meet the standards specified in this procedure, or granted an exception by the IT Department, are approved for connectivity to a Lakemary network.

6.3 Scope

All employees, contractors, consultants, temporary and other workers at Lakemary, including all personnel affiliated with third parties that maintain a wireless infrastructure device on behalf of Lakemary must adhere to this procedure. This procedure applies to all wireless infrastructure devices that connect to a Lakemary network or reside on a Lakemary site that provide wireless connectivity to endpoint devices including, but not limited to, laptops, desktops, cellular phones, and tablets. This includes any form of wireless communication device capable of transmitting packet data.

6.4 Procedure

6.4.1 General Requirements

All wireless infrastructure devices that reside at a Lakemary site and connect to a Lakemary network, or provide access to information classified as Lakemary Confidential, or above must:

- Abide by the standards specified in the Wireless Infrastructure Standard.
- Be installed, supported, and maintained by the IT Department.
- Use Lakemary approved authentication protocols and infrastructure.
- Use Lakemary approved encryption protocols.
- Maintain a hardware address (MAC address) that can be registered and tracked.

6.4.2 Home Wireless Device Requirements

6.4.2.1 Wireless infrastructure devices that provide direct access to the Lakemary corporate network, must conform to the Home Wireless Device Requirements as detailed in the Wireless Infrastructure Standard.

6.4.2.2 Wireless infrastructure devices that fail to conform to the Home Wireless Device Requirements must be installed in a manner that prohibits direct access to the Lakemary corporate network. Access to the Lakemary corporate network through this device must use standard remote access authentication.

6.5 Procedure Compliance

6.5.1 Compliance Measurement

The IT Department will verify compliance to this procedure through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the procedure owner.

6.5.2 Exceptions

Any exception to the procedure must be approved by the IT Department in advance.

6.5.3 Non-Compliance

An employee found to have violated this procedure may be subject to disciplinary action, up to and including termination of employment.

6.6 Related Standards, Policies and Processes

- Wireless Infrastructure Standard

6.7 Definitions and Terms

The following definition and terms can be found in the SANS Glossary located at: https://www.sans.org/security-resources/glossary-of-terms/

- MAC Address

7 Data Classification and Standards

7.1 Overview

Data assets are some of the most valuable assets owned by Lakemary (LMC). LMC produces, collects, and uses many different types of data in fulfilling its mission. Laws mandate privacy and protection of certain types of data, and LMC's need to manage the risks to its reputation and to its clients requires the protection of other information. Classifying data is the first step in determining the data's need for protection.

7.2 Purpose

The purpose of this standard is intended to help LMC employees classify data for the purposes of determining its need for protection and determining applicable policies and laws.

7.3 Scope

This standard can be used to classify any data that are stored, processed, or transmitted by LMC. The standard applies to all types of data:

- Electronic Data
- Data recorded on paper
- Information shared orally, visually or by other means

7.4 Standard

7.4.1 Classification

Data can be classified either in terms of its need for protection (e.g., Sensitive Data) or in terms of its need for availability (e.g., Critical Data). To classify data in terms of its need for protection, use section 7.4.1.1 of this standard. To classify data in terms or its availability needs, use section 7.4.1.2 of this standard.

7.4.1.1 Classifying Data According to Protection Needs

Match any data that need to be classified to the one of the four categories which best describes its need for confidentiality and its risk profile. The four categories are Public, Internal, Sensitive, and Restricted.

7.4.1.1.1 Public Data - Data can be disclosed without restriction. Examples - Directories, Maps, Syllabi and Course Materials, de-identified data sets, etc.

7.4.1.1.2 Internal Data - Confidentiality of data is preferred, but information contained in data may be subject to open records disclosure. Examples - email correspondence, budget plans, etc.

7.4.1.1.3 Sensitive Data - Data confidentiality required by law, policy, or contractual obligation.

Characteristics of Sensitive Data

- Compliance Risk: Protection of data is mandated by law (e.g., HIPAA) or required by private contract (e.g., non-disclosure agreements).
- Reputation Risk: Loss of confidentiality or integrity will cause significant damage to LMC's reputation. For example, loss of social security numbers or defacement of the LMC website would likely be a news item that would appear in the media.
- Other Risks: Loss of confidentiality that could cause harm to individuals such as LMC clients, personnel, donors and partners. Loss of confidentiality or integrity that would cause LMC to incur significant costs in response.
- Treatment in Open Records Requests: Sensitive information is typically redacted from open records disclosures.

Examples of Sensitive Data

- Student records and prospective student records (w/o Social Security Numbers)
- Donor records
- Critical infrastructure information (physical plant detail, IT systems information, system passwords, information security plans, etc.)
- Research information related to sponsorship, funding, human subject, etc.
- Information protected by non-disclosure agreements (NDAs) or similar private contracts
- Law enforcement and investigative records

7.4.1.1.4 Restricted Data - Restricted data requires privacy and security protections. Special authorization may be required for use and collection. Examples - data sets with individual Social Security Numbers (or last four of SSN), credit card transaction or cardholder data, patient health data, financial data, etc.

Characteristics of Restricted Data

- Chief Program Officer Approval: LMC Chief Program Officer or their designees must authorize all storing, processing, and transmitting of Restricted Information.
- Compliance Risk: Protection of information is mandated by law (e.g., HIPAA) or required by private contract.
- Reputation Risk: Loss of confidentiality or integrity will cause significant damage to LMC's reputation.
- Other Risks: Loss of the confidentiality or integrity of the information that could cause harm to individuals and cause LMC to incur significant costs in response.
- Treatment in Open Records Requests: Records with restricted information are typically not open for public inspection.

Examples of Restricted Data

- Social Security Numbers (or last four numbers of an individual's SSN)
- Credit/debit card data
- Protected Healthcare Information (PHI)
- Financial account data

7.4.1.2 Classifying Data According to Availability Needs

Match any data that need to be classified according to availability needs to the one of the three categories which best describes its need for availability needs. The three categories are Supportive, High-Priority, and Critical.

7.4.1.2.1 Supportive Data - Supportive data is necessary for day-to-day operations but is not critical to LMC's core functions. Examples - course materials, meeting minutes, workstation images, etc.

7.4.1.2.2 High-priority Data - Availability of data is necessary for departmental function. Destruction or temporary loss of data may have an adverse effect on a department's mission but would not affect company-wide function.

7.4.1.2.3 Critical Data - Critical data has the highest need for availability. If the information is not available due to system downtime, modification, destruction, etc., LMC's functions and mission would be impacted. The availability of this information must be rigorously protected.

Characteristics of Critical Data

- Mission Risk: Short-term or prolonged loss of availability could prevent LMC from accomplishing its core functions or mission.
- Health and Safety Risk: Loss of availability may create health or safety risk for individuals. (e.g., emergency notification data, health data).
- Compliance Risk: Availability of information is mandated by law (e.g., HIPAA) or required by private contract.
- Reputation Risk: Loss of data will cause significant damage to LMC's reputation.

Examples of Critical Data

- Emergency notification/contact data
- Protected Healthcare Information (PHI)
- Student records

7.4.2 Protection

See the table below for minimum standard protection requirements for each category of data when being used or handled in a specific context (e.g., Sensitive Data sent in an email message). Please note that the below protection standards are not intended to supersede any regulatory or contractual requirements for handling data. Some specific data sets, such as student records data, credit/debit card data, healthcare data, and financial account data, may have stricter requirements in addition to the minimum standard requirements listed below.

	Public Data	Internal Data	Sensitive Data	Restricted Data
Collection and Use	No protection requirements	No protection requirements	Limited to authorized users as outlined in the LMC Privacy Standard.	SSNs and PHI may not be used to identify members of the LMC community if there is a reasonable alternative. SSNs shall not be used as a username or password. SSNs shall not be collected on unauthenticated individuals. All credit/debit card uses must be approved by the LMC Controller.
Granting Access or Sharing	No protection requirements	Reasonable methods shall be used to ensure internal data is accessed by or shared with authorized	Access shall be limited to authorized LMC officials or agents with a legitimate interest and a need to know as	Access shall be limited to authorized LMC officials or agents with a legitimate interest and a need to know as

	Public Data	Internal Data	Sensitive Data	Restricted Data
		individuals or individuals with a legitimate need to know.	outlined in the *LMC Privacy Standard*. Per LMC Requirements, all access shall be approved by an appropriate data owner and tracked in a manner sufficient to be auditable. Before granting access to external third parties, contractual agreements which outline responsibilities for security of the data shall be approved by the IT Department	outlined in the *LMC Privacy Standard*. Per LMC Requirements, all access shall be approved by an appropriate data owner and tracked in a manner sufficient to be auditable. Before granting access to external third parties, contractual agreements which outline responsibilities for security of the data shall be approved by the IT Department
Disclosure, Public Posting, etc.	No protection requirements	Reasonable methods shall be used to ensure internal data is accessed by or shared with authorized individuals or individuals with a legitimate need to know.	Sensitive data shall not be disclosed without consent. Sensitive data may not be posted publicly. Directory information can be disclosed without consent. However, per FERPA, individuals can opt out of	Not permitted unless required by law.

	Public Data	Internal Data	Sensitive Data	Restricted Data
			directory information disclosure	
Electronic Display	No protection requirements	Reasonable methods shall be used to ensure internal data is accessed by or shared with authorized individuals or individuals with a legitimate need to know.	Only to authorized and authenticated users of a system.	Restricted data shall be displayed only to authorized and authenticated users of a system. Identifying numbers or account number shall be, at least partially, masked or redacted.
Open Records Requests	Data can be readily provided upon request. However, individuals who receive a request must coordinate with LMC management before providing data.	Individuals who receive a request must coordinate with LMC management.	Sensitive data is typically not subject to open records disclosure. However, some open records requests can be fulfilled by redacting sensitive portions of records. Individuals who receive a request must coordinate with LMC Officers.	Restricted data is typically not subject to open records disclosure. However, some open records requests can be fulfilled by redacting sensitive portions of records. Individuals who receive a request must coordinate with LMC Officers.
Exchanging with Third Parties, Service Providers, Cloud Services, etc.	No protection requirements	Reasonable methods shall be used to ensure that the third party's responsibilities for confidentiality /	A contractual agreement outlining security responsibilities shall be in place and approved by LMC before exchanging data	A contractual agreement outlining security responsibilities shall be in place and approved by LMC before exchanging data

	Public Data	Internal Data	Sensitive Data	Restricted Data
		privacy of the data are defined and documented.	with the third party / service provider.	with the third party / service provider.
Storing or Processing: Server Environment	Servers that connect to the LMC Network shall comply with the *Server Security Standard*.	Servers that connect to the LMC Network shall comply with the *Server Security Standard*.	Servers shall comply with security requirements as outlined in the *Server Security Standard*.	Servers shall comply with security requirements as outlined in the *Server Security Standard*. Storing Credit/Debit card Primary Account Number (PAN) data is not permitted.
Storing or Processing: Endpoint Environment (e.g., laptop, phone, desktop, tablet)	Systems that connect to the LMC Network shall comply with *Workstation Security for HIPPA Standard*.	Systems that connect to the LMC Network shall comply with *Workstation Security for HIPPA Standard*.	Systems shall comply with security requirements as outlined in the *Workstation Security for HIPPA Standard*.	Workstations shall comply with security requirements as outlined in the *Workstation Security for HIPPA Standard*. Storing PHI or PAN data is not permitted. Storing restricted data on personally-owned devices is not permitted.
Storing on Removable Media (e.g., flash drives, DVD's)	No protection requirements	No protection requirements	Sensitive data shall only be stored on removable media in an encrypted	Not permitted unless required by law.

	Public Data	Internal Data	Sensitive Data	Restricted Data
			file format or within an encrypted volume.	If required by law, data stored on removable media shall be encrypted and the media shall be stored in a physically secured environment. Storing restricted data on personally owned media is not permitted.
Electronic Transmission	No protection requirements	No protection requirements	Data shall be transmitted in either an encrypted file format or over a secure protocol or connection.	Secure, authenticated connections or secure protocols shall be used for transmission of restricted data.
Email and other electronic messaging	No protection requirements	Reasonable methods shall be used to ensure internal data is only included in messages to authorized individuals or individuals with a legitimate need to know.	Sensitive data shall only be included in messages within an encrypted file attachment. Messages shall only be sent to authorized individuals or other individuals with a legitimate need to know.	Not permitted unless required by law. If required by law, data shall be included in an encrypted file attached to the message or via email security service (ESS).
Printing, mailing, fax, etc.	No protection requirements	Reasonable methods shall be used to	Printed materials that include sensitive data	Printed materials that include restricted data

	Public Data	Internal Data	Sensitive Data	Restricted Data
		ensure that printed materials are only distributed or available to authorized individuals or individuals with a legitimate need to know.	shall only be distributed or available to authorized individuals or individuals with a legitimate need to know. Access to any area where printed records with sensitive data are stored shall be limited by the use of controls (e.g., locks, doors, monitoring) sufficient to prevent unauthorized entry.	shall only be distributed or available to authorized individuals or individuals with a legitimate need to know. Access to any area where printed records with restricted data are stored shall be limited by the use of controls (e.g., locks, doors, monitoring) sufficient to prevent unauthorized entry.
Disposal	No protection requirements	No protection requirements	Data shall be deleted and unrecoverable (e.g., eraser, zero-fill, DoD multipass). Physical media (e.g., paper, CD) should be destroyed so that data on the media cannot be recovered or reconstructed.	Data shall be deleted and unrecoverable (e.g., eraser, zero-fill, DoD multipass). Physical media (e.g., paper, CD) should be destroyed so that data on the media cannot be recovered or reconstructed.

7.5 Standard Compliance

7.5.1 Compliance Measurement

The IT Department team will verify compliance to this Standard through various methods, including but not limited to, business tool reports, internal and external audits.

7.5.2 Exceptions

Any exception to the Standard must be approved by the IT Department in advance.

7.5.3 Non-Compliance

An employee found to have violated this Standard may be subject to disciplinary action, up to and including termination of employment.

7.6 Related Standards and Processes

- Workstation Security for HIPAA Standard
- Minimum Access Standard
- Server Security Standard

7.7 Definitions and Terms

- FERPA (Family Educational Rights and Privacy Act), http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html

8 Wireless Infrastructure Standard

8.1 Overview

See Purpose.

8.2 Purpose

This standard specifies the technical requirements that wireless infrastructure devices must satisfy to connect to a Lakemary network. Only those wireless infrastructure devices that meet the requirements specified in this standard or are granted an exception by the IT Department are approved for connectivity to a Lakemary network.

8.2.1 Device requirements

Network devices including, but not limited to, hubs, routers, switches, firewalls, remote access devices, modems, or wireless access points, must be installed, supported, and maintained by the IT Department or an approved support organization.

8.3 Scope

All employees, contractors, consultants, temporary and other workers at Lakemary and its subsidiaries, including all personnel that maintain a wireless infrastructure device on behalf of Lakemary, must comply with this standard. This standard applies to wireless devices that make a connection the network and all wireless infrastructure devices that provide wireless connectivity to the network.

The IT Department must approve exceptions to this standard in advance.

8.4 Standard

8.4.1 General Requirements

All wireless infrastructure devices that connect to a Lakemary network or provide access to Lakemary Confidential, Lakemary Highly Confidential, or Lakemary Restricted information must:

- Use Extensible Authentication Protocol-Fast Authentication via Secure Tunneling (EAP-FAST), Protected Extensible Authentication Protocol (PEAP), or Extensible Authentication Protocol-Translation Layer Security (EAP-TLS) as the authentication protocol.
- Use Advanced Encryption Standard (AES) protocol with a minimum key length of 128 bits.
- All Bluetooth devices must use Secure Simple Pairing with encryption enabled.

8.4.2 Home Wireless Device Requirements

All home wireless infrastructure devices that provide direct access to a Lakemary network, such as those using VPN, must adhere to the following:

- Enable Wi-Fi Protected Access 2 (WPA2)
- Change the default SSID name
- Change the default login and password

8.5 Policy Compliance

8.5.1 Compliance Measurement

The IT Department will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

8.5.2 Exceptions

Any exception to the policy must be approved by the IT Department in advance.

8.5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

8.6 Related Standards, Policies and Processes

- Lab Security Policy

8.7 Definitions and Terms

The following definition and terms can be found in the SANS Glossary located at: https://www.sans.org/security-resources/glossary-of-terms/

- AES
- EAP-FAST
- EAP-TLS
- PEAP
- SSID
- TKIP
- WPA2

9 Remote Access Standard

9.1 Overview

Remote access to our corporate network is essential to maintain our Team’s productivity, but in many cases, this remote access originates from networks that may already be compromised or are at a significantly lower security posture than our corporate network. While these remote networks are beyond the control of Lakemary, we must mitigate these external risks the best of our ability.

9.2 Purpose

The purpose of this standard is to define rules and requirements for connecting to Lakemary's network from any host. These rules and requirements are designed to minimize the potential exposure to Lakemary from damages, which may result from unauthorized use of Lakemary resources. Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical Lakemary internal systems, and fines or other financial liabilities incurred as a result of those losses.

9.3 Scope

This standard applies to all Lakemary employees, contractors, vendors and agents with a Lakemary-owned or personally-owned computer or workstation used to connect to the Lakemary network. This standard applies to remote access connections used to do work on behalf of Lakemary, including reading or sending email and viewing intranet web resources. This standard covers any and all technical implementations of remote access used to connect to Lakemary networks.

9.4 Standard

It is the responsibility of Lakemary employees, contractors, vendors and agents with remote access privileges to Lakemary's corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to Lakemary.

General access to the Internet for business use through the Lakemary network is strictly limited to Lakemary employees, contractors, vendors and agents (hereafter referred to as “Authorized Users”). When accessing the Lakemary network from a personal computer, Authorized Users are responsible for preventing access to any Lakemary computer resources or data by non-Authorized Users. Performance of illegal activities through the Lakemary network by any user (Authorized or otherwise) is prohibited. The Authorized User bears responsibility for and consequences of misuse of the Authorized User’s access. For further information and definitions, see the *Acceptable Use Standard*.

Authorized Users will not use Lakemary networks to access the Internet for outside business interests.

For additional information regarding Lakemary's remote access connection options, including how to obtain a remote access login, free anti-virus software, troubleshooting, etc., contact the IT Department.

9.4.1 Requirements

9.4.1.1 Secure remote access must be strictly controlled with encryption (i.e., Virtual Private Networks (VPNs)) and strong passwords or pass-phrases. For further information, see the Acceptable Encryption Standard and the Password Construction Guidelines.

9.4.1.2 Multi-Factor Authentication (MFA) must be used when making any remote connection.

9.4.1.3 While using a Lakemary-owned computer to remotely connect to Lakemary's corporate network, Authorized Users shall ensure the remote host is not connected to any other network at the same time, with the exception of personal networks that are under their complete control or under the complete control of an Authorized User or Third Party.

9.4.1.4 Use of external resources to conduct Lakemary business must be approved in advance by the IT Department and the appropriate business unit manager.

9.4.1.5 All hosts that are connected to Lakemary internal networks via remote access technologies must use the most up-to-date anti-virus, which will be installed with the VPN client, this includes personal computers. Third party connections must comply with requirements as stated in the Third Party Agreement.

9.4.1.6 Personal equipment used to connect to Lakemary's networks must meet the requirements of Lakemary-owned equipment for remote access (see *BYOD Standard*).

9.5 Standard Compliance

9.5.1 Compliance Measurement

The IT Department will verify compliance to this standard through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and inspection, and will provide feedback to the standard owner and appropriate business unit manager.

9.5.2 Exceptions

Any exception to the standard must be approved by Remote Access Services and the IT Department in advance.

9.5.3 Non-Compliance

An employee found to have violated this standard may be subject to disciplinary action, up to and including termination of employment.

9.6 Related Standards, Policies and Processes

Please review the following policies for details of protecting information when accessing the corporate network via remote access methods, and acceptable use of Lakemary's network:

- *Acceptable Encryption Standard*
- *Acceptable Use Standard*
- *Password Construction Guidelines*
- *Password Protection Standard*
- *BYOD Standard*

10 Remote Access Tools Standard

10.1 Overview

Remote desktop software, also known as remote access tools, provide a way for computer users and support staff alike to share screens, access work computer systems from home, and vice versa. Examples of such software include LogMeIn, GoToMyPC, Citrix, and Windows Remote Desktop (RDP). While these tools can save significant time and money by eliminating travel and enabling collaboration, they also provide a back door into the Lakemary network that can be used for theft of, unauthorized access to, or destruction of assets. As a result, only approved, monitored, and properly controlled remote access tools may be used on Lakemary computer systems.

10.2 Purpose

This standard defines the requirements for remote access tools used at Lakemary.

10.3 Scope

This standard applies to all remote access where either end of the communication terminates at a Lakemary computer asset.

10.4 Standard

All remote access tools used to communicate between Lakemary assets and other systems must comply with the following standard requirements.

10.4.1 4.1 Remote Access Tools

Lakemary provides mechanisms to collaborate between internal users, with external partners, and from non-Lakemary systems. The approved software list can be obtained from the IT Department. Because proper configuration is important for secure use of these tools, mandatory configuration procedures are provided for each of the approved tools.

The approved software list may change at any time, but the following requirements will be used for selecting approved products:

a) All remote access tools or systems that allow communication to Lakemary resources from the Internet or external partner systems must require at a minimum user name and password authentication.
b) The authentication database source must be Active Directory, and the authentication protocol must involve a challenge-response protocol that is not susceptible to replay attacks. The remote access tool must mutually authenticate both ends of the session.
c) Remote access tools must support the Lakemary application layer proxy rather than direct connections through the perimeter firewall(s).
d) Remote access tools must support strong, end-to-end encryption of the remote access communication channels as specified in the Lakemary network encryption protocols standard.

e) All Lakemary antivirus, data loss prevention, and other security systems must not be disabled, interfered with, or circumvented in any way.
f) All remote access tools must be purchased through the standard Lakemary procurement process, and the IT Department must approve the purchase.

10.5 Standard Compliance

10.5.1 Compliance Measurement

The IT Department will verify compliance to this standard through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the standard owner.

10.5.2 Exceptions

Any exception to the standard must be approved by the IT Department in advance.

10.5.3 Non-Compliance

An employee found to have violated this standard may be subject to disciplinary action, up to and including termination of employment.

10.6 Related Standards, Policies and Processes

None.

10.7 Definitions and Terms

The following definition and terms can be found in the SANS Glossary located at: https://www.sans.org/security-resources/glossary-of-terms/

- Application layer proxy

11 Technology Equipment Disposal Standard

11.1 Overview

Technology equipment often contains parts which cannot simply be thrown away. Proper disposal of equipment is both environmentally responsible and often required by law. In addition, hard drives, USB drives, CD-ROMs and other storage media contain various kinds of Lakemary data, some of which is considered sensitive. To protect our constituent's data, all storage mediums must be physical destroyed or properly erased before being disposed of. However, simply deleting or even formatting data is not considered sufficient. When deleting files or formatting a device, data is marked for deletion, but is still accessible until being overwritten by a new file. Therefore, special tools must be used to securely erase data prior to equipment disposal.

11.2 Purpose

The purpose of this standard it to define the guidelines for the disposal of technology equipment and components owned by Lakemary.

11.3 Scope

This standard applies to any computer/technology equipment or peripheral devices that are no longer needed within Lakemary including, but not limited to the following: personal computers, servers, hard drives, laptops, mainframes, smart phones, or handheld computers (i.e., Windows Mobile, iOS or Android-based devices), peripherals (i.e., keyboards, mice, speakers), printers, scanners, typewriters, compact and floppy discs, portable storage devices (i.e., USB drives), backup tapes, printed materials.

All Lakemary employees and affiliates must comply with this standard.

11.4 Standard

11.4.1 Technology Equipment Disposal

11.4.1.1 When Technology assets have reached the end of their useful life, they should be sent to the IT Department for proper disposal.

11.4.1.2 The IT Department will ensure physical destruction or securely erase all storage mediums in accordance with current industry best practices.

11.4.1.3 If wiping data, all data including all files and licensed software shall be removed from equipment using disk-sanitizing software that cleans the media overwriting each and every disk sector of the machine.

11.4.1.4 No computer or technology equipment may be sold to any individual other than through the processes identified in this standard (Section 11.4.2 below).

11.4.1.5 No computer equipment should be disposed of via skips, dumps, landfill etc. Electronic equipment should be returned to the IT Department. The IT Department will properly remove all data prior to final disposal, and/or physically be rendered unreadable (Section 11.4.1.6 below).

11.4.1.6 All electronic drives must be degaussed or overwritten with a commercially available disk-cleaning program. Hard drives may also be removed and rendered unreadable (drilling, crushing or other demolition methods).

11.4.1.7 Computer Equipment refers to desktop, laptop, tablet or netbook computers, printers, copiers, monitors, servers, handheld devices, telephones, cell phones, disc drives or any storage device, network switches, routers, wireless access points, batteries, backup tapes, etc.

11.4.1.8 Technology equipment with non-functioning memory or storage technology will have the memory or storage device removed and it will be physically destroyed.

11.5 Standard Compliance

11.5.1 Compliance Measurement

The IT Department will verify compliance to this standard through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the standard owner.

11.5.2 Exceptions

Any exception to the standard must be approved by the IT Department in advance.

11.5.3 Non-Compliance

An employee found to have violated this standard may be subject to disciplinary action, up to and including termination of employment.

11.6 Related Standards, Policies and Processes

None.

11.7 Definitions and Terms

None.

12 BYOD Standard

12.1 Overview

This document provides standards and rules of behavior for the use of personally owned smart phones and/or tablets by Lakemary employees to access Lakemary resources and/or services, a practice commonly referred to as Bring Your Own Device (BYOD). Access to and continued use of Lakemary resources is granted on condition that each user reads, signs, respects, and follows Lakemary standards concerning the use of these resources and/or services. This standard is intended to protect the security and integrity of Lakemary data and technology infrastructure. Limited exceptions to the policy may occur due to variations in devices and platforms.

14.1.1 Expectation of Privacy

Lakemary will respect the privacy of your personal device and will only request access to the device by technicians to implement security controls or to respond to legitimate discovery requests arising out of administrative, civil, or criminal proceedings. This differs from policy for Lakemary provided equipment and/or services, where employees do not have the right, nor should they have the expectation, of privacy while using equipment and/or services.

12.2 Purpose

The purpose of these guidelines is to provide best practices for the use of personal devices on the Lakemary network.

12.3 Scope

These guidelines apply to employees, contractors, consultants, temporary and other workers at Lakemary, including all personnel affiliated with third parties.

12.4 Acceptable Use

- See *Acceptable Use Standard*

12.5 Security

- In order to prevent unauthorized access, devices must be password protected or use biometrics (e.g., fingerprint reader) using the features of the device.
- The company's strong password policy is: Passwords must be at least eight characters and a combination of upper- and lower-case letters, numbers and special characters. Passwords will be rotated every 90 days and the new password cannot be one of 10 previous passwords.
- The device must lock itself with a password, PIN or biometrics if it is idle for ten minutes.
- The device must be locked while unattended.

- No PHI or Lakemary proprietary data shall be stored on the device.
- The device will have Anti-Malware software (e.g., Malwarebytes) installed and programmed to scan once per week.
- Rooted (Android) or jailbroken (iOS) devices are strictly forbidden from accessing the network.
- Smartphones and tablets that are not on the company's list of supported devices are not allowed to connect to the internal network.
- Smartphones and tablets belonging to employees that are for personal use only are not allowed to connect to the internal network.
- Employees' access to company data is limited based on user profiles defined by IT and automatically enforced.
- The employee's device may be remotely wiped if:
    - The device is lost or stolen.
    - The employee terminates his or her employment.
    - IT detects a data or policy breach, a virus or similar threat to the security of the company's data and technology infrastructure.

12.6 Risks/Liabilities/Disclaimers

- While IT will take every precaution to prevent the employee's personal data from being lost in the event it must remote wipe a device, but it is the employee's responsibility to take additional precautions, such as backing up email, contacts, etc.
- Lakemary reserves the right to disconnect devices or disable services without notification.
- Lost or stolen devices must be reported to the company within 24 hours. Employees are responsible for notifying their mobile carrier immediately upon loss of a device.
- The employee is expected to use his or her devices in an ethical manner at all times and adhere to the company's acceptable use policy as outlined above.
- The employee is personally liable for all costs associated with his or her device.
- The employee assumes full liability for risks including, but not limited to, the partial or complete loss of company 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.
- Lakemary reserves the right to take appropriate disciplinary action up to and including termination for noncompliance with this policy.

12.7 Policy Compliance

The IT Department will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

12.7.1 Exceptions

Any exception to this standard must be approved by the IT Department in advance.

12.7.2 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

12.8 Related Standards, Policies and Processes

None.

12.9 Definitions and Terms

None.

13 Revision History

Date of Change	Responsible	Summary of Change
25 November 2015	IT Department	Modified for Lakemary, based on SANS Institute standard template.
30 December 2015	IT Department	Added sections for introduction and employee agreement
12 June 2017	IT Department	• Added BYOD standard. • Changed password length requirements from 15 to 8 characters, minimum.
1 May 2019	IT Department	• Updated section 5.4.11 of email standard to specify access outside of Lakemary LAN. • Updated restricted data email transmission standard in section 8.4.2 Protection.
20 July 2020	IT Department	Updated format and various grammar issues.
7 October 2020	IT Department	Added HIPAA audit policy statement.
17 August 2021	IT Department	Updated section 12 Technology Equipment Disposal Standard
3 September 2023	IT Department	• Combined Password Creation and Password Protection Guidelines • Removed HIPAA Data Audit Policy • Added MFA guidelines to Email and Remote Access Guidelines • Removed Employee Purchase of Disposed Equipment

14 Employee Agreement

The undersigned employee hereby acknowledges that he/she has received a copy of the Technology Standards and Procedures Handbook for Lakemary.

The employee further understands and agrees that:

- ❖ The handbook is intended to be a general guide to the technology standards and procedures of Lakemary and is not an employment agreement or a guarantee of employment.
- ❖ The employee is an at-will employee, meaning that both the employee and Lakemary may terminate the employment relationship at any time, with or without cause or advance notice. The employee´s at-will status can only be changed through a written employment contract that is authorized and signed by the Company President. Any oral statements, promises, or other contracts are hereby deemed invalid.
- ❖ Lakemary reserves the right to make changes to the employment handbook without prior notice.

I acknowledge receipt of the Lakemary's Technology Standards and Procedures Handbook and understand that it is up to me to read and familiarize myself with its contents. I have read and understood all of the above information, and I acknowledge my at-will employment status.

Employee Signature ____

Print Name ____

Date ____________________________________