LKP Securities Ltd

Cyber Security and Cyber Resilience Policy

Version: 1.0
Author: Ketan Shah
Date : 31st Jan 2019

Version	Author	Status	Date	Reason
1	Ketan Shah	Under Review	18th Feb 2019	First Edition

Reviewed By

Ketan Shah
Chief Technology Officer

Reviewed & Approved By

Pratik Doshi
Managing Director

Board of Directors (09-Feb-2019)

Contents

Purpose

This policy defines the technical controls and security configurations users and Information Technology (IT) administrators are required to implement in order to ensure the integrity and availability of the data environment at LKP Securities Limited, hereinafter, referred to as the "LKP".

Practice

It serves as a central policy document with which all employees and contractors must be familiar, and defines actions and prohibitions that all users must follow. The policy provides IT managers within LKP with policies and guidelines concerning the acceptable use of LKP technology equipment, e-mail, Internet connections, voice-mail, facsimile, future technology resources and information processing.

The policy requirements and restrictions defined in this document shall apply to network infrastructures, databases, external media, encryption, hardcopy reports, films, slides, models, wireless, telecommunication, conversations, and any other methods used to convey knowledge and ideas across all hardware, software, and data transmission mechanisms. This policy must adhered by all LKP employees or temporary workers at all locations and by contractors working with LKP as subcontractors.

Scope

This policy document defines common security requirements for all LKP personnel and systems that create, maintain, store, access, process or transmit information. This policy also applies to information resources owned by others, such as contractors of LKP, entities in the private sector, in cases where LKP has a legal, contractual or fiduciary duty to protect said resources while in LKP custody. In the event of a conflict, the more restrictive measures apply. This policy covers LKP network system, which is comprised of various hardware, software, communication equipment and other devices designed to assist LKP in the creation, receipt, storage, processing, and transmission of information. This definition includes equipment connected to any LKP domain or VLAN, either hardwired or wirelessly, and includes all stand-alone equipment that is deployed by LKP at its office locations or at remote locales.

Acronyms / Definitions

Common terms and acronyms that may be used this document.

M.D. (Managing Director) / CEO (Chief Executive Officer) - The M.D. or CEO is responsible for the overall privacy and security practices of the company.

CTO – The Chief Technology Officer / Head of IT

DO – The Designated Officer is responsible for annual security training of all staff on confidentiality issues.

CST – Confidentiality and Security Team

Encryption – The process of transforming information, using an algorithm, to make it unreadable to anyone other than those who have a specific 'need to know.'

External Media –i.e. CD-ROMs, DVDs, floppy disks, flash drives, USB keys, thumb drives, tapes, etc.

SOW - Statement of Work - An agreement between two or more parties that details the working relationship between the parties and lists a body of work to be completed.

User - Any person authorized to access an information resource.

VPN – Virtual Private Network – Provides a secure passage through the public Internet.

Designated Officer
Designated Officer will oversee all ongoing activities related to the development, implementation, and maintenance of LKP privacy policies in accordance with applicable federal and state laws. Details of the current Designated Officer as approved by the board of directors on 4th February 2019:

Name	:	Ms. Sunita Ambavkar
Contact Number	:	+91 9619266687
Email Id	:	sunita@lkpsec.com

CST : Confidentiality / Security Team (CST) / Technology Committee
LKP has established a Confidentiality / Security Team made up of key personnel whose responsibility it is to identify areas of concern within LKP and act as the first line of defense in enhancing the appropriate security posture.

All members identified within this policy are assigned to their positions by the Board of Directors. The term of each member assigned is at the discretion of the Board of Directors. This committee will consist of the positions within LKP most responsible for the overall security policy planning of the organization- the M.D., CEO, DO and the CTO (where applicable).

The current members of the CST are:
Name : Mr. Dinesh Waghela
Name : Ms. Sunita Ambavkar
Name : Mr. Ketan Shah

The CST will meet Half Yearly to discuss security issues and to review concerns that arose during the year. The CST will identify areas that needs be addressed during annual training and review/update security policies as necessary. The CST will address security issues as they arise and recommend and approve immediate security actions to be undertaken. It is the responsibility of the CST to identify areas of concern within LKP and act as the first line of defense in enhancing the security posture of LKP.

The CST is responsible for maintaining a log of security concerns or confidentiality issues. This log must be maintained on a routine basis, and must include the dates of an event, the actions taken to address the event, and recommendations for personnel actions, if appropriate. This log will be reviewed during the half yearly meetings.

The Designated Officer (DO) or other assigned personnel is responsible for maintaining a log of security enhancements and features that have been implemented to further protect all sensitive information and assets held by LKP.

Employee Responsibilities
Employee Requirements

The first line of defense in data security is the individual LKP user. LKP users are responsible for the security of all data which may come to them in whatever format. LKP is responsible for maintaining ongoing training programs to inform all users of these requirements.

Challenge Unrecognized Personnel **-** It is the responsibility of all LKP personnel to take positive action to provide physical security. If you see an unrecognized person in a restricted LKP office location, you should challenge them as to their right to be there. All visitors to LKP offices must sign in at the front desk. In addition, all visitors must wear a visitor/contractor badge. All other personnel must be employees of LKP. Any challenged person who does not respond appropriately should be immediately reported to admin staff.

Secure Laptop **-** When out of the office all laptop computers must be secured by keeping it in a locked drawer. Most LKP computers will contain sensitive data of either business or financial nature, and the utmost care should be taken to ensure that this data is not compromised. Laptop computers are unfortunately easy to steal, particularly during the stressful period while traveling.

Unattended Computers **-** Unattended computers should be locked by the user when leaving the work area. This feature is discussed with all employees during training. Employees are not allowed to take any action which would override this setting.

Home Use of LKP Corporate Assets - Only computer hardware and software owned by and installed by LKP is permitted to be connected to or installed on LKP equipment. Only software that has been approved for corporate use by LKP may be installed on LKP equipment. Personal computers supplied by LKP are to be used solely for business purposes. All employees and contractors must read and understand the list of prohibited activities that are outlined below. Modifications or configuration changes are not permitted on computers supplied by the LKP for home use.

Retention of Ownership - All software programs and documentation generated or provided by employees, consultants, or contractors for the benefit of LKP are the property of LKP unless covered by a contractual agreement. Nothing contained herein applies to software purchased by LKP employees at their own expense.

Prohibited Activities

Personnel are prohibited from the following activities. The list is not inclusive. Other prohibited activities are referenced elsewhere in this document.

Attempting to break into an information resource or to bypass a security feature - This includes running password-cracking programs or sniffer programs, and attempting to circumvent file or other resource permissions.

Introducing, or attempting to introduce, computer viruses, Trojan horses, peer-to-peer ("P2P") or other malicious code into an information system.

Exception: Authorized information system support personnel, or others authorized by LKP Designated Officer, may test the resiliency of a system. Such personnel may test for susceptibility to hardware or software failure, security against hacker attacks, and system infection.

Browsing. The willful, unauthorized access or inspection of confidential or sensitive information to which you have not been approved on a "need to know" basis is prohibited. LKP has access to customers information which is protected by SEBI regulations which stipulate a "need to know" before approval is granted to view the information. The purposeful attempt to look at or access information to which you have not been granted access by the appropriate approval procedure is strictly prohibited.

Personal or Unauthorized Software. Use of personal software is prohibited. All software installed on LKP computers must be approved by LKP.

Software Use. Violating or attempting to violate the terms of use or license agreement of any software product used by LKP is strictly prohibited.

System Use. Engaging in any activity for any purpose that is illegal or contrary to the policies, procedures or business interests of LKP is strictly prohibited.

Electronic Communication, E-mail, Internet Usage

As a productivity enhancement tool, LKP encourages the business use of electronic communications. However, all electronic communication systems and all messages generated on or handled by LKP owned equipment are considered the property of LKP – not the property of individual users. Consequently, this policy applies to all LKP employees and contractors, and covers all electronic communications including, but not limited to, telephones, e-mail, voice mail, instant messaging, Internet, fax, personal computers, and servers.

LKP provided resources, such as individual computer workstations or laptops, computer systems, networks, e-mail, and Internet software and services are intended for business purposes. Access to external email services like gmail, yahoo, etc. are strictly prohibited. However, incidental personal use is permissible as long as:

- it does not consume more than a trivial amount of employee time or resources,
- it does not interfere with staff productivity,
- it does not preempt any business activity,
- it does not violate any of the following:

Copyright violations – This includes the act of pirating software, music, books and/or videos or the use of pirated software, music, books and/or videos and the illegal duplication and/or distribution of information and other intellectual property that is under copyright.

Illegal activities – Use of LKP information resources for or in support of illegal purposes as defined by federal, state or local law is strictly prohibited.

Commercial use – Use of LKP information resources for personal or commercial profit is strictly prohibited.

Political Activities – All political activities are strictly prohibited on LKP premises. LKP encourages all of its employees to vote and to participate in the election process, but these activities must not be performed using LKP assets or resources.

Harassment – LKP strives to maintain a workplace free of harassment and that is sensitive to the diversity of its employees. Therefore, LKP prohibits the use of computers, e-mail, voice mail, instant messaging, texting and the Internet in ways that are disruptive, offensive to others, or harmful to morale. For example, the display or transmission of sexually explicit images, messages, and cartoons is strictly prohibited. Other examples of misuse includes, but is not limited to, ethnic slurs, racial comments, off-color jokes, or anything that may be construed as harassing, discriminatory, derogatory, defamatory, threatening or showing disrespect for others.

Junk E-mail - All communications using IT resources shall be purposeful and appropriate. Distributing "junk" mail, such as chain letters, advertisements, or unauthorized solicitations is prohibited. A chain letter is defined as a letter sent to several persons with a request that each send copies of the letter to an equal number of persons. Advertisements offer services from someone else to you. Solicitations are when someone asks you for something. If you receive any of the above, delete the e-mail message immediately. Do not forward the e-mail message to anyone.

Generally, while it is **NOT** the policy of the LKP to monitor the content of any electronic communication, LKP is responsible for servicing and protecting the LKP's equipment, networks, data, and resource availability and therefore may be required to access and/or monitor electronic communications from time to time. Several different methods are employed to accomplish these goals. For example, an audit or cost analysis may require reports that monitor phone numbers dialed, length of calls, number of calls to / from a specific handset, the time of day, etc. Other examples where electronic communications may be monitored include, but are not limited to, research and testing to optimize IT resources, troubleshooting technical problems and detecting patterns of abuse or illegal activity.

LKP reserves the right, at its discretion, to review any employee's files or electronic communications to the extent necessary to ensure all electronic media and services are used in compliance with all applicable laws and regulations as well as LKP policies.

Employees should structure all electronic communication with recognition of the fact that the content could be monitored, and that any electronic communication could be forwarded, intercepted, printed or stored by others.

Internet Access

Internet access is provided for LKP users and is considered a great resource for the organization. This resource is costly to operate and maintain, and must be allocated primarily to those with business, administrative or contract needs. The Internet access provided by LKP should not be used for entertainment, listening to music, viewing the sports highlight of the day, games, movies, etc. While seemingly trivial to a single user, the company wide use of these non-business sites consumes a huge amount of Internet bandwidth, which is therefore not available to responsible users.

Users must understand that individual Internet usage is monitored, and if an employee is found to be spending an excessive amount of time or consuming large amounts of bandwidth for personal use, disciplinary action will be taken.

Many Internet sites, such as games, peer-to-peer file sharing applications, chat rooms, and on-line music sharing applications, have already been blocked by the LKP routers and firewalls. This list is constantly monitored and updated as necessary. Any employee visiting pornographic sites will be disciplined and may be terminated.

Reporting Software Malfunctions

Users should inform the appropriate LKP IT personnel when the user's software does not appear to be functioning correctly. The malfunction - whether accidental or deliberate - may pose an information security risk. If the user, or the user's manager or supervisor, suspects a computer virus infection, LKP computer these steps should be taken immediately:

- Stop using the computer
- Do not carry out any commands, including commands to <Save> data.
- Do not close any of the computer's windows or programs.
- Do not turn off the computer or peripheral devices.
- If possible, physically disconnect the computer from networks to which it is attached.
- Inform the appropriate personnel as soon as possible. Write down any unusual behavior of the computer (screen messages, unexpected disk access, unusual responses to commands) and the time when they were first noticed.
- Write down any changes in hardware, software, or software use that preceded the malfunction.
- Do not attempt to remove a suspected virus!

The IT team should monitor the resolution of the malfunction or incident, and report to the CST the result of the action with recommendations on action steps to avert future similar occurrences.

Report Security Incidents

It is the responsibility of each LKP employee or contractor to report perceived security incidents on a continuous basis to the appropriate supervisor or IT person. A User is any person authorized to access an information resource. Users are responsible for the day-to-day, hands-on security of that resource. Users are to formally report all security incidents or violations of the security policy immediately to the

Designated Officer. Users should report any perceived security incident to either their immediate supervisor, or to their department head, or to any member of the LKP CST. Members of the CST are specified above in this document.

Reports of security incidents shall be escalated as quickly as possible. Each member of the LKP CST must inform the other members as rapidly as possible. Each incident will be analyzed to determine if changes in the existing security structure are necessary. All reported incidents are logged and the remedial action indicated. It is the responsibility of the CST to provide training on any procedural changes that may be required as a result of the investigation of an incident.

Security breaches shall be promptly investigated. If criminal action is suspected, the LKP Designated Officer shall contact the appropriate law enforcement and investigative authorities immediately, which may include but is not limited to the police.

Transfer of Sensitive/Confidential Information

When confidential or sensitive information from one individual is received by another individual while conducting official business, the receiving individual shall maintain the confidentiality or sensitivity of the information in accordance with the conditions imposed by the providing individual. All employees must recognize the sensitive nature of data maintained by the LKP and hold all data in the strictest confidence. Any purposeful release of data to which an employee may have access is a violation of LKP policy and will result in personnel action, and may result in legal action.

Transferring Software and Files between Home and Work

Personal software shall not be used on LKP computers or networks. If a need for specific software exists, submit a request to your supervisor or department head. Users shall not use LKP purchased software on home or on non-LKP computers or equipment.

LKP proprietary data, including but not limited to patient information, IT Systems information, financial information or human resource data, shall not be placed on any computer that is not the property of the LKP without written consent of the respective supervisor or department head. It is crucial for LKP to protect all data and, in order to do that effectively we must control the systems in which it is contained. In the event that a supervisor or department head receives a request to transfer LKP data to a non-LKP Computer System, the supervisor or department head should notify the Designated Officer or appropriate personnel of the intentions and the need for such a transfer of data in a written form.

The LKP Wide Area Network ("WAN") is maintained with a wide range of security protections in place, which include features such as virus protection, e-mail file type restrictions, firewalls, anti-hacking hardware and software, etc. Since LKP does not control non-LKP personal computers, LKP cannot be sure of the methods that may or may not be in place to protect LKP sensitive information, hence the need for this restriction. However, limited access can be granted basis of the approval from the department head, designated office or any member of CST.

Internet Considerations

Special precautions are required to block Internet (public) access to LKP information resources not intended for public access, and to protect confidential LKP information when it is to be transmitted over the Internet.

The following security and administration issues shall govern Internet usage. Prior approval of LKP Designated Officer or appropriate personnel authorized by the LKP shall be obtained before:

- An Internet, or other external network connection, is established;
- LKP information (including notices, memoranda, documentation and software) is made available on any Internet-accessible computer (e.g. web or ftp server) or device;
- Users may not install or download any software (applications, screen savers, etc.). If users have a need for additional software, the user is to contact their supervisor;
- Use shall be consistent with the goals of the LKP. The network can be used to market services related to the LKP, however use of the network for personal profit or gain is prohibited.
- Confidential or sensitive data - including credit card numbers, telephone calling card numbers, logon passwords, and other parameters that can be used to access goods or services - shall be encrypted before being transmitted through the Internet.
- The encryption software used, and the specific encryption keys (e.g. passwords, pass phrases), shall be escrowed with the LKP Designated Officer or appropriate personnel, to ensure they are safely maintained/stored. The use of encryption software and keys, which have not been escrowed as prescribed above, is prohibited, and may make the user subject to disciplinary action.

Identification and Authentication

Passwords

User Account Passwords

User ids and passwords are required in order to gain access to all LKP networks and workstations. This means that all passwords must conform to restrictions and limitations that are designed to make the password difficult to guess. Users are required to select a password in order to obtain access to any electronic information both at the server level and at the application level. When passwords are reset, the user will be automatically prompted to manually change that assigned password. LKP follows a Password policy consists of:

- Login Attempt
- Minimum password length
- Passwords must meet complexity requirements
- Maximum password length

Confidentiality Agreement

Users of LKP information resources shall acknowledge following statement:

I understand that any unauthorized use or disclosure of information residing on the LKP information resource systems may result in disciplinary action consistent with the policies and procedures of legal agencies.

Access Control

Information resources are protected by the use of access control systems. Access control systems include both internal (passwords, encryption, access control lists, constrained user interfaces) and external (port protection devices, firewalls, host-based authentication).

Rules for access to resources (including internal and external telecommunications and networks) have been established by the information/application owner or manager responsible for the resources.

Network Connectivity

Permanent Connections

The security of LKP systems can be jeopardized from third party locations if security practices and resources are inadequate. When there is a need to connect to a third party location, a risk analysis should be conducted. The risk analysis should consider the type of access required the value of the information, the security measures employed by the third party, and the implications for the security of LKP systems. The Designated Officer or appropriate personnel should be involved in the process, design and approval.

Firewalls

Authority from the Designated Officer or appropriate personnel must be received before any employee or contractor is granted access to a LKP router or firewall.

Antivirus Software Installation

Antivirus software is installed on all LKP personal computers and servers. Virus update patterns are updated daily on the LKP servers and workstations. Virus update engines and data files are monitored by appropriate administrative staff that is responsible for keeping all virus patterns up to date.

Configuration - The antivirus software currently implemented by LKP is Kaspersky Endpoint Security. Updates are received directly from Kaspersky which is scheduled daily at 5:00 PM.

Remote Deployment Configuration - Through an automated procedure, updates and virus patches may be pushed out to the individual workstations and servers on an as needed basis.

Monitoring/Reporting – A record of virus patterns for all workstations and servers on the LKP network may be maintained. Appropriate administrative staff is responsible for providing reports for auditing and emergency situations as requested by the Designated Officer or appropriate personnel.

New Software Distribution

Only software created by LKP application staff, if applicable, or software approved by the Designated Officer or appropriate personnel will be used on internal computers and networks. A list of approved software is as follows:

For all Employees:

- Microsoft Windows 7 and Above
- Ubuntu 17.10 and higher
- Microsoft Office 2007 standard and above
- Open office
- Web Browsers
- LD (All Version)
- Adobe Reader
- Anydesk
- Ammyadmin
- Kaspersky Anti-Virus
- WinRAR

Risk, Dealers & Research:

- Trading software's
- NSE Neat or any latest release from NSE
- NSE NOW or any latest release from NSE
- BSE Bolt or any latest release from BSE
- MCX Trader Workstation or any latest release from MCX
- NCDEX – Nextra or any latest release from NCDEX
- Odin
- Bloomberg
- Cashcow
- Charting Software (subject to approval from IT and business)
- Hawkeye

All new software will be tested by appropriate personnel in order to ensure compatibility with currently installed software and network configuration. In addition, appropriate personnel must scan all software for viruses before installation.

All data and program files that have been electronically transmitted to a LKP computer or network from another location must be scanned for viruses immediately after being received. Contact the appropriate LKP personnel for instructions for scanning files for viruses. Every diskette, CD-ROM, DVD and USB device is a potential source for a computer virus. Therefore, every diskette, CD-ROM, DVD and USB device must be scanned for virus infection prior to copying information to a LKP computer or network. Computers shall never be "booted" from a diskette, CD-ROM, DVD or USB device received from an outside source. Users shall always remove a USB device from the computer when not in use.

Retention of Ownership

All software programs and documentation generated or provided by employees, consultants, or contractors for the benefit of LKP are the property of LKP unless covered by a contractual agreement. Employees developing programs or documentation must sign a statement acknowledging LKP

ownership at the time of employment. Nothing contained herein applies to software purchased by LKP employees at their own expense.

Server Room Security

It is the policy of LKP to provide Server room access in a secure manner. All other facilities, if applicable, have similar security appropriate for that location.

Only specific LKP employees are given the security code for server room entrance. Disclosure of the security card to non-employees is strictly prohibited.

The door to the server room area is locked at all times and requires appropriate access card. Swipe cards control access to the server room doors. Each cards is coded to allow admission to specific areas based on each individual's job function or need to know. The office is equipped with security cameras to record activities in entire office and the server room. All the activities in this area is recorded on a 24x7 basis.

VPN and Firewall Protections

VPN and Firewall Use**:** Established procedures must be rigidly followed when accessing LKP core infrastructure from outside of any type. The users require the use of VPN software and firewall devices.

Data Security Protection

Data Backup**:** Backup procedures have been established that encrypt the data being moved to an external media. Use only that procedure – do not create one on your own. If there is not a backup procedure established or if you have external media that is not encrypted, contact the appropriate LKP personnel for assistance. Protect external media by keeping it in your possession when traveling.

Transferring Data to LKP**:** Transferring of data to the LKP requires the use of an approved VPN connection to ensure the confidentiality and integrity of the data being transmitted. Do not circumvent established procedures, nor create your own method, when transferring data to or from LKP.

External System Access: If you require access to an external system, contact your supervisor or IT Team. Designated Officer or appropriate personnel will assist in establishing a secure method of access to the external system.

E-mail:

User the Email services for the business purpose only. Do not access any external email services like gmail, yahoo, etc. as they are not permitted unless approved by LKP.

Non-LKP Networks: Extreme care must be taken when connecting LKP equipment to a home or hotel network. Although LKP actively monitors its security status and maintains organization wide protection policies to protect the data within all contracts, LKP has no ability to monitor or control the security procedures on non-LKP networks.

Protect Data in Your Possession: View or access only the information that you have a need to see to complete your work assignment. Regularly review the data you have stored in the local system or shared drive to ensure that old and junk data is eliminated as soon as possible.

Data Entry When in a Public Location: Do not perform work tasks which require the use of sensitive corporate or customer level information when you are in a public area, i.e. airports, airplanes, hotel lobbies. Computer screens can easily be viewed from beside or behind you.

Specific Protocols and Devices

Wireless Usage Standards and Policy

Due to an emergence of wireless access points in hotels, airports, and in homes, it has become imperative that a Wireless Usage policy be developed and adopted to ensure the security and functionality of such connections for LKP employees. This policy outlines the processes and procedures for acquiring wireless access privileges, utilizing wireless access, and ensuring the security of LKP laptops and mobile devices. Only Mobile devices of the department heads will be mapped with the Corporate Wi-Fi. A prior approval of department and Designated Officer or appropriate personnel is required for any exceptions.

Approval Procedure – Employees issued with permanent company laptop are eligible for Wi-Fi access at the time of issuance. In order to be granted the ability to utilize the wireless network interface on your LKP laptop issued for temporary purpose or mobile device you will be required to gain the approval of your immediate supervisor or department head and the Designated Officer or appropriate personnel of LKP.

Software Requirements - The following is a list of minimum software requirements for any LKP laptop that is granted the privilege to use wireless access:

- Latest windows update
- Antivirus software
- Appropriate VPN Client, if applicable
- Internet Explorer 8 or Greater

If your laptop does not have all of these software components, please notify your supervisor or IT so these components can be installed.

Disposal of External Media / Hardware

Disposal of External Media

It must be assumed that any external media in the possession of an employee is likely to contain either confidential or other sensitive information. Accordingly, external media (CD-ROMs, DVDs, diskettes, USB drives) should be disposed of in a method that ensures that there will be no loss of data and that the confidentiality and security of that data will not be compromised.

The following steps must be adhered to:

- It is the responsibility of each employee to identify media which should be shredded and to utilize this policy in its destruction.

- External media should never be thrown in the trash.
- When no longer needed all forms of external media are to be sent to the Designated Officer or appropriate personnel for proper disposal.

Requirements Regarding Equipment

All equipment to be disposed of will be wiped of all data, and all settings and configurations will be reset to factory defaults. No other settings, configurations, software installation or options will be made. Asset tags and any other identifying logos or markings will be removed.

Disposition of Excess Equipment

As the older LKP computers and equipment are replaced with new systems, the older machines are held in inventory for a wide assortment of uses:

- Older machines are regularly utilized for spare parts.
- Older machines are used on an emergency replacement basis.
- Older machines are used for testing new software.
- Older machines are used as backups for other production equipment.
- Older machines are used when it is necessary to provide a second machine for personnel who travel on a regular basis.

Violations

Listed below are the types of violations that require sanctions to be applied. They are stated at levels 1, 2, and 3 depending on the seriousness of the violation.

Level	Description of Violation
1	• Accessing information that you do not need to know to do your job. • Sharing computer access codes (user name & password). • Disclosing sensitive information with unauthorized persons. • Copying sensitive information without authorization. • Changing sensitive information without authorization. • Discussing sensitive information in a public area or in an area where the public could overhear the conversation. • Discussing sensitive information with an unauthorized person. • Failing/refusing to cooperate with the Information Security Officer, Designated Officer, Chief Technology Officer, and/or authorized designee.
2	• Second occurrence of any Level 1 offense (does not have to be the same offense). • Unauthorized use or disclosure of sensitive information. • Using another person's computer access code (user name & password). • Failing/refusing to comply with a remediation resolution or recommendation.
3	• Third occurrence of any Level 1 offense (does not have to be the same offense). • Second occurrence of any Level 2 offense (does not have to be the same offense). • Obtaining sensitive information under false pretenses.

	• Using and/or disclosing sensitive information for commercial advantage, personal gain, or malicious harm.

Recommended Disciplinary Actions

In the event that a workforce member violates LKP's privacy and security policies or related laws governing the protection of sensitive and customer identifiable information, the following recommended disciplinary actions will apply.

Violation Level	Recommended Disciplinary Action
1	• Verbal or written reprimand • Retraining on privacy/security awareness • Retraining on LKP's privacy and security policies • Retraining on the proper use of internal or required forms
2	• Letter of Reprimand*; or suspension • Retraining on privacy/security awareness • Retraining on LKP's privacy and security policies • Retraining on the proper use of internal or required forms
3	• Termination of employment or contract • Civil penalties or other applicable law • Criminal penalties or other applicable law

Important Note: The recommended disciplinary actions are identified in order to provide guidance in policy enforcement and are not meant to be all-inclusive. If formal discipline is deemed necessary, LKP shall consult with Human Resources prior to taking action. When appropriate, progressive disciplinary action steps shall be followed allowing the employee to correct the behavior which caused the disciplinary action.

*A Letter of Reprimand must be reviewed by Human Resources before given to the employee.

Exceptions

Depending on the severity of the violation, any single act may result in disciplinary action up to and including termination of employment or contract with LKP.