

Information Security Policy

Version:	1.0
Date of version:	11/11/2025
Created by:	LBC Enterprises B.V.
Approved by:	Ian Parke (MD)
Confidentiality level	Confidential – Internal Use

Change History

Version	Date	Author	Comment
1.0			Initial Release - Draft
1.1	11/11/2025	Complaine	V1

Table of Contents

1.	Information Security Policy	4
1.1	Introduction	4
1.2	Objectives	4
1.3	Scope	5
1.4	Policy Statement	5
1.5	Responsibilities	5
1.6	Enforcement	6
1.7	Standard	6
2.	Data Ownership and Classification Policy	7
2.1	Purpose	7
2.2	Policy Responsibilities	7
2.3	Assigning of Ownership	7
2.4	Data Classification	7
2.5	Measures for Data Protection	8
3.	System and Networks	9
3.1	Prohibited Activity	9
3.2	Physical Security	10
4.	Electronic Mail (Email) Policy	11
4.1	Ownership	11
4.2	Usage	11
4.4	Conformity	12
5.	Internet Security	12
5.1	Ownership	12
5.2	Usage	12
5.3	Browsing not Work Related	13
6.	User Management	13
6.1	Entry/Access to the System	13
6.2	Identification	13
6.3	Verification	13
6.4	Authorisation	13
6.5	User Access Termination	14
6.6	Various Access Control	14
6.6.1	Dormant Inactive Accounts	14
6.6.2	Automatic Log-Off	14

6.6.3	Unsuccessful Login Attempts	15
7.	Password Policy.....	15
7.1	Ownership	15
7.2	Password Administration	15
7.3	Configuration	15
7.4	Responsibilities and Maintenance.....	16
7.5	Important Passwords	16
7.6	Monitoring.....	16
7.7	System Security.....	16
8.	Clean Desk & Computer Use	16
8.1	Clean Desk Policy	17
8.2	Equipment Use	17
9.	Portable Media and Equipment	18
9.1	Adherence to the Policy.....	18
10.	Destruction of Media and Equipment.....	19
10.1	Media Disposal	19
10.2	Equipment Disposal	19
11.	Anti-Virus Protection.....	19
11.1	Adherence to Policy.....	19
12.	Intrusion Prevention	20
13.	Training.....	20

1. Information Security Policy

1.1 Introduction

This policy outlines comprehensive guidelines regarding the use of email, internet, laptops, and portable devices, among other directives that employees must thoroughly review. The company's internet and intranet systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts for electronic mail, internet browsing, and file transfer protocols (FTP), as well as any related documentation such as reports, are considered company property. These resources are intended strictly for business purposes, supporting the company's and its clients' or customers' interests during regular operations.

1.2 Objectives

Information security is a vital asset of LBC Enterprises B.V. and it is essential to implement appropriate measures to safeguard information assets such as data, whether in digital or

physical formats, as well as networks and computer systems. These measures are necessary to prevent the loss of confidentiality, availability, and integrity of information. The objective of this policy is to ensure that these three critical aspects of information are consistently protected:

- Confidentiality: Ensuring that information is accessible only to those authorized to have access.
- Integrity: Information should be correct; unauthorised persons should not be able to alter the information.
- Availability: Information should always be available to authorised persons.

1.3 Scope

This policy encompasses all information managed by the company, whether stored on computer systems or in any other format. It applies to all employees and individuals working with the company, regardless of their position, location, or relationship with the organization.

1.4 Policy Statement

It is the Company's policy to ensure that:

- Information will be safeguarded against unauthorized access.
- Confidentiality of information will be ensured.
- The integrity of information will be preserved.
- Compliance with regulatory and legislative requirements will be maintained.
- Continuity plans will be developed, tested, and upheld.
- Information security awareness will be promoted among all staff.
- All actual or suspected information security breaches will be reported to and investigated by designated security personnel.
- Intellectual property copyrights will be respected.
- Information will be protected against malicious code.

1.5 Responsibilities

The Chief Executive Officer (CEO) and Compliance Officer have primary responsibility for maintaining the policy and offering advice and guidance on information security and its implementation. The CTO and middle management are tasked with enforcing this policy within their respective business areas and ensuring that all employees understand their duty to protect the company's assets and adhere to security standards and procedures.

Employees have specific responsibilities, including:

- Exercising good judgment regarding the reasonable use of company resources; if uncertain, they should consult their direct supervisor.
- Conducting themselves ethically at all times.
- Avoiding the misuse of data or information obtained through their role.
- Not exploiting any discovered system weaknesses.
- Performing their duties diligently and being accountable for any misuse of the company's computer systems.

- Clarifying the classification of information when its confidentiality is unclear.
- Reporting any known violations or system weaknesses to the designated security personnel or their line manager.
- Reporting all intrusions or suspicions, assisting in investigations, and adhering to the Incident Response Policy.

1.6 Enforcement

Failure to comply with this policy will result in a disciplinary review by management. Appropriate actions will be taken in accordance with the company's disciplinary procedures.

1.7 Standard

All related policies, along with supporting standards, procedures, guidelines, and operating instructions issued to support this policy statement, are integral components of the Corporate Information Security Policy Statement. These documents shall be utilized as standards to be implemented by the CEO/CTO. Additionally, they will serve as a basis for compliance monitoring and review.

2. Data Ownership and Classification Policy

2.1 Purpose

Data is one of the company's most valuable assets and must be used responsibly and ethically. Proper classification of the company's data is essential to ensure that appropriate security measures are implemented. Additionally, assigning clear responsibilities for handling all data is necessary so that these security measures can be effectively implemented and monitored.

2.2 Policy Responsibilities

Data Owners

Data Owners are responsible for understanding and classifying all data under their control. They ensure that appropriate security measures are applied based on the data classification and that these measures comply with legal requirements. Data Owners have the exclusive authority to grant access to the data and determine the access rights for individuals.

Data Custodians/Processors

Data Custodians or Processors are responsible for the data entrusted to them, regardless of the format, for specific periods. They must maintain the required level of security to protect the data during their custodianship. IT Support personnel are typical examples of Data Custodians.

Data Users

Data Users are granted access rights to data by the Data Owners to perform their duties. Users must not misuse these rights and may only perform actions authorized by the Data Owners.

Management

Management is responsible for appointing Data Owners and Custodians. This is done after gaining a thorough understanding of the data and the roles of the individuals involved.

2.3 Assigning of Ownership

The company retains ultimate ownership of the data. However, it delegates responsibility and authority over the data to relevant company departments and/or authorities as needed. This approach recognizes that ownership responsibility is not a singular, absolute concept, but rather consists of a range of responsibilities.

2.4 Data Classification

This policy defines the adherence to the data classification standard, specifies the responsibilities of department employees in relation to the standard, and offers guidelines for the classification of data.

Classification	Description	Data Type
Confidential	Data whose loss, corruption or unauthorised disclosure would be a violation of laws and regulations, even if the disclosure	Sensitive employee data includes information such as criminal records, medical histories, and political affiliations. Sensitive

	is only internal within the Company.	customer data comprises employee payroll details, banking information, employment contracts, non-public financial data of the company, user credentials, business strategies, intellectual property, confidential source code, CCTV recordings, and office alarm codes.
Secret	Data that, if lost, corrupted, or disclosed without authorization, could harm the company's business operations, image, reputation, or research capabilities, and potentially lead to financial or legal losses. This data constitutes the primary focus of the company's operations and is typically familiar to employees within specific departments or projects.	Source code, marketing strategies, essential customer details, fundamental employee records, and data stored on the intranet server within departmental or segregated directories.
Internal	Information intended for general employee awareness. Data where potential loss, corruption, or unauthorized disclosure would not inherently lead to business, financial, or legal repercussions.	Information stored in public folders on the intranet server, the internal directory of contact information, company policies and procedures, and guidelines.
Public	Data that does not fit into any of the other specified data classifications below. This information can be publicly released and shared with third parties.	The company's registered location, permit and license details, publicly available website content, marketing materials, and press releases.

Data will be categorized as Internal, Restricted, or Confidential whenever feasible. Public data does not require labeling.

This list is not exhaustive, and additional data may be classified as Confidential, Restricted, Internal, or Public. If there is uncertainty regarding the classification of a specific type of data not listed here, it should always be handled as Confidential until classified by the responsible asset owner.

2.5 Measures for Data Protection

Class	Measures	Type of Authorisation Required
Confidential	Data must be encrypted using the most robust techniques available for both storage and transmission.	Access to this information, whether by third parties or internal personnel, must always adhere strictly to a need-

	Additionally, networks or databases containing such information should be isolated from other networks.	to-know and least privilege basis, approved by the data owner.
Secret	It should be subjected to the same level of control as internal data. Moreover, if this data is transmitted over a public network, it must be encrypted to maintain confidentiality. All data transmissions must be encrypted at all times.	Access to this information by third parties must always be granted strictly on a need-to-know and least privilege basis, approved by either the data custodian or the data owner. Internal access will follow the same criteria and may be authorized by a line manager or department head.
Internal	The availability and integrity of the data must be safeguarded during both transmission and storage. Encryption is not mandatory for internal transmission, but access to this data must be controlled through authentication measures.	Third-party access necessitates permission from the data custodian or data owner. Internal users do not require authorization for disclosure.
Public	Does not require specific protection measures during storage or transmission.	No authorization is necessary for internal or third-party disclosure.

3. System and Networks

Authorized individuals within the Company may monitor equipment, systems, and network traffic at any time for security and network maintenance purposes. While the Company endeavors to uphold a reasonable level of privacy, users should be aware that any data they generate on the Company's systems remains the property of the Company. Due to the necessity of safeguarding the Company's network, the Company cannot ensure the confidentiality of employees' information stored on any network device owned by the Company.

The Company also reserves the right to conduct periodic audits of networks and systems to verify compliance with this policy.

3.1 Prohibited Activity

The following activities are strictly prohibited without exceptions:

- Violating the rights of any individual or company protected by copyright, trade secret, patent, or other intellectual property laws. This includes installing or distributing "pirated" or unauthorized software products not properly licensed for use by or authorized for use by the Company.
- Unauthorized copying of copyrighted materials, including digitizing and distributing photographs from magazines, books, or other copyrighted sources, copyrighted music, and installing any copyrighted software without an active license from the Company or end user.

- Exporting software, technical information, encryption software, or technology in violation of international export control laws is illegal. Consultation with appropriate management is required before exporting any questionable material.
- Introducing malicious programs into the network or server, such as viruses, worms, Trojan horses, or email bombs, is strictly prohibited.
- Disclosing account credentials to others or permitting others, including family members or household members when working from home, to use your account is prohibited.
- Transferring sensitive data between office and home equipment without authorization from management is prohibited.
- Using Company computing assets to engage in the procurement or transmission of material that violates sexual harassment or hostile workplace laws in the user's local jurisdiction is strictly prohibited.
- Making fraudulent offers of products, items, or services originating from a Company account is prohibited.
- Making warranty statements, express or implied, unless it is part of normal job duties, is not permitted.
- Engaging in security breaches or disruptions of network communication, including accessing data not intended for the employee, logging into unauthorized servers or accounts, and causing disruptions such as network sniffing, denial of service attacks, or forged routing information for malicious purposes, is strictly prohibited.
- Conducting port scanning or security scanning without prior approval from management is expressly prohibited.
- Conducting any form of network monitoring that intercepts data not intended for the employee's host, unless part of regular job duties, is prohibited.
- Circumventing user authentication or security measures on any host, network, or account is prohibited.
- Interfering with or denying service to any user or host other than the employee's own, such as conducting denial of service attacks, is strictly prohibited.
- Using any program, script, command, or sending messages with the intent to interfere with or disable a user's terminal session via any means, locally or over the Internet/Intranet/Extranet, is prohibited.
- Providing information about or lists of the Company's employees or Account Holders to external parties.
- Removing or physically tampering with equipment, or allowing unauthorized physical access to Company equipment, is strictly prohibited.

3.2 Physical Security

Proper measures concerning access control, environmental safety, and protection are essential to safeguard the Company's equipment from physical harm, tampering, and unauthorized removal.

- Office premises must feature structurally sound walls, windows, and doors to enhance security.
- At the end of each day, windows and doors will be securely locked. Responsibility for this task rests with the last person leaving the building, who is also accountable for arming any intrusion detection or burglar alarms.

- Visitors must be accompanied at all times by a staff member while on the premises.
- Key technical equipment will be housed in an ISO/IEC 27001 certified data center to ensure optimal security and operational standards.
- Servers designated for office use will be located in a secure, locked room free from environmental hazards. Regular inspections and maintenance will be conducted to prevent equipment failures.
- Network cables, power lines, and telecommunication connections will be shielded to prevent external interference or damage.
- Backup media will be stored in locations free from potential hazards such as strong magnets, spills, or other environmental risks.

4. Electronic Mail (Email) Policy

The primary objective of email usage is to facilitate the Company's daily operations. This section details the Company's policy regarding employee obligations concerning electronic mail (email) messages transmitted or received through the Company's email systems. It pertains to both internal and external network systems and services that the Company may utilize.

4.1 Ownership

All email equipment and messages within the Company's email system are considered the property of the Company. This includes any messages created, sent, or received using these systems, which are also regarded as Company property. The Company reserves the right to access and disclose the contents of these messages to relevant entities as necessary. This policy ensures that email communications are managed in accordance with company guidelines and regulatory requirements.

4.2 Usage

- All email communications must adhere to the same standards as letters, faxes, memos, or other official business correspondence.
- Confidential or Restricted data, including attachments, must not be transmitted in clear text over the Internet to clients or colleagues.
- No copyrighted or proprietary information may be distributed via the Company's email system without approval from a Director, Compliance Officer, or line manager.
- Commercial messages, employee solicitations, or messages of a religious or political nature are prohibited from being distributed using the Company's email.
- Bulk forwarding of jokes, chain letters, or similar materials, especially to recipients outside the office, is not permitted.
- Urgent virus warnings should be forwarded to the IT department for verification, as many such warnings are often hoaxes.
- Employees should exercise caution and avoid downloading attachments or following hyperlinks in emails where the authenticity of the message and identity of the sender cannot be confirmed.
- Employees must refrain from executing attachments to emails if they are executable files (e.g., *.exe, *.vbs, *.com, .swf) regardless of the email's source, due to potential risks such as viruses, email bombs, or Trojan horse code.

- Email messages must not contain offensive or disruptive content, including but not limited to obscene language, harassing images or language, comments or images based on race, ethnicity, sexual orientation, religion, or political beliefs.
- Employees are not permitted to access or read email messages that were not specifically sent to them unless authorized by the Company or the email recipient.
- Any attempt to conceal the sender's identity or misrepresent oneself in email or electronic communications is strictly prohibited.
- Posting from Company email addresses to newsgroups, chat rooms, forums, or social media platforms is strictly prohibited unless it is part of official business duties.

4.3 Emails not Business Related

Limited and sporadic personal use of email is allowed. These messages are considered Company property and must adhere to the same guidelines as any other business-related email.

4.4 Conformity

Failure to comply with this policy may lead to disciplinary measures, including termination and potential legal action if deemed necessary. Employees are encouraged to promptly report any misuse of the Company's email system or violations of this policy to the designated authority. The identity of those reporting such incidents will be kept strictly confidential at all times. It is important for employees to understand that misuse of computers constitutes a criminal offense, and they should be mindful of the associated consequences.

5. Internet Security

This section outlines the Company's policy on employee responsibilities for Internet usage over Company's network. The purpose of providing employees with access to the Internet is to conduct the required day-to-day business of the Company.

5.1 Ownership

The Company asserts ownership over all computers and network components, including any installed software and data stored on computers, devices, media, or the network. To ensure proper use when accessing the internet, the Company reserves the right to conduct checks on computers, network devices, and audit logs. Other forms of computer usage are governed by separate policies. Employees are required to promptly report any violations of this policy to the designated Information Security personnel. The confidentiality of employees reporting violations will be strictly maintained at all times.

5.2 Usage

All employees requiring access to Internet services must use Company-approved software and Internet gateways. When data requires more than just a password for protection, encryption should be applied using secure algorithms and proper key management practices as needed. Accessing illicit, hacker, or suspicious websites is strictly forbidden. Employees are prohibited from downloading any software or executable files. It's important to note that web browsers track visited sites. Technicians needing access to potentially dubious sites for security

monitoring or vulnerability assessments must obtain explicit permission. Such access must occur from systems devoid of sensitive data, and technicians must exercise utmost caution throughout.

5.3 Browsing not Work Related

Any such browsing can take place during breaks, however, the usage rules above will still be applicable.

6. User Management

We will implement User Management controls in our system to serve two main purposes: first, to prevent unauthorized access by intruders; and second, to restrict authorized users to their specific and legitimate purposes. This policy applies universally to all employees, contractors, account holders, and any other entities needing access to Company data or systems, regardless of their location or the form in which they interact with our systems.

6.1 Entry/Access to the System

This will be accomplished by mandating that users log into the system by entering a User ID or Username recognized by the system, followed by a password or passphrase to verify their identity as the rightful owner of the User ID. Users must complete the log-on process before engaging with the system in any manner.

6.2 Identification

A User ID typically comprises a non-secret sequence of characters and is typically the initial information a user inputs to "log on" or gain access to a system. To safeguard both the user and the Company, each User ID must be unique to the individual and should never be shared or disclosed to others, whether during the user's tenure with the company or afterwards. Access to a User ID for any Company system should only be granted to individuals with a verified need to use the system and who have undergone proper identification and authorization procedures.

6.3 Verification

Prior to logging onto a system and accessing resources, the user's identity must undergo authentication to prevent impersonation. While passwords are suitable for internal networks, they may not provide adequate security in high-risk environments. It is recommended to implement multi-factor authentication where feasible and supported to enhance security measures.

6.4 Authorisation

Access to system resources must be granted based on the user or process requiring access. Users with higher privilege levels may authorize access rights to resources they control for other users or processes, always adhering to the principle of least privilege or 'need to know'. Access rights to data files should be determined solely by the content and the user's role. Additionally, access to other resources such as terminals, printers, and network services must be carefully restricted. It is especially important to limit the use of commands like system

administrator, security administrator, and database administrator to a select few users and terminals.

Before granting authorization to access any resource, the following steps must be completed:

- Clearly identify the specific resources each individual or group needs access to, specifying the level of access required (e.g., READ and/or WRITE), and considering future access needs.
- Standardize user identifiers and task names to reflect the respective Company section where the data owner operates.
- Establish naming standards for files and other resources based on the involved processes, departments/units, or individuals.

6.5 User Access Termination

Upon the conclusion of an employee's tenure with the company, it is the responsibility of the Director CTO to ensure that the employee's account is promptly closed or disabled across all relevant systems. This includes notifying third-party platforms if the employee had access privileges there. Additionally, all relevant correspondence pertaining to the employee should be meticulously archived and retained for future reference and auditing purposes.

6.6 Various Access Control

6.6.1 Dormant Inactive Accounts

Inactive or improperly privileged accounts should not remain on a system as they pose a potential risk for misuse. Measures to address this should involve implementing the following controls:

- Disabling vendor accounts originally used for system setup or changing their passwords, especially when initial passwords are widely known.
- Establishing procedures that allow users to request temporary suspension and subsequent reinstatement of their access rights, accommodating situations such as leave.

6.6.2 Automatic Log-Off

All PCs, laptops, workstations, and web applications within the company must adhere to stringent security protocols. This includes implementing password-protected screensavers with an automatic activation feature set to activate after 30 minutes or less of inactivity. Alternatively, users must log off when leaving their workstations unattended to prevent unauthorized access. The automatic disablement of logged-on workstations should be configured through group policy where available, or locally on the machine if group policy settings are not accessible. This requirement applies to laptops as well, where applicable.

In addition to these automatic security measures, back-office systems will automatically log off after one hour (60 minutes) of inactivity, with the possibility of stricter policies depending on specific security requirements. The automatic screen lock feature must prompt users to re-enter their credentials upon activation.

6.6.3 Unsuccessful Login Attempts

Protection against brute-force attacks will be implemented by configuring the login procedure to lock out or suspend any user who enters an incorrect password a set number of times. The maximum number of allowable attempts before triggering a logout should range between 3 to 6, depending on the security risk associated with the system or the data being accessed. Alternatively, account throttling may be employed as an additional measure to deter brute-force attacks.

Furthermore, access to user accounts should only be granted upon successful authentication. Automatic re-enabling of accounts after a predefined period should be strictly prohibited to enhance security measures and prevent unauthorized access attempts.

7. Password Policy

Passwords are utilized to verify the identity of users seeking access to a system, necessitating their secure construction and maintenance at all times. Users encompass not only employees and customers of the company but also all management personnel, contractors, auditors, and any other third parties granted access to the systems. It is crucial that passwords are managed in a manner that ensures their confidentiality and integrity to safeguard against unauthorized access and potential security breaches.

7.1 Ownership

Each system user must have a unique password that remains the sole property of the assigned user. Under no circumstances should passwords be shared to gain access to the system. Users are accountable for selecting strong passwords that align with this policy's requirements. Administrators and Application Owners are responsible for ensuring that all applications and systems enforce robust password standards.

7.2 Password Administration

Since each password is owned by the individual user and serves as the gateway to system access, users bear the responsibility of ensuring that their password composition and upkeep align with this policy. By doing so, users contribute to enhancing the security of the company's systems, making it more challenging for potential wrongdoers to compromise them.

7.3 Configuration

- The minimum password length for normal users must be at least 8 characters.
- Passwords must include characters from at least three of the following categories:
 - uppercase letters,
 - lowercase letters,
 - numbers, and
 - special characters.
- Avoid using repetitive sequences like "ABCD," "1111," or "1234."

The Company promotes the use of password managers, allowing employees to avoid using the same password across multiple applications. When creating passwords, choose ones that

are easy to remember but avoid using dictionary words, telephone numbers, family names, license plate numbers, simple words with numbers, or any form of your User ID.

7.4 Responsibilities and Maintenance

- Passwords should be changed at least every 60 days for high-risk systems, and between 120 to 180 days for lower-risk systems; consult the system owner or IT team if unsure.
- Avoid reusing passwords until at least 4 password changes have been completed.
- Do not write down passwords in any form.
- Immediately change assigned passwords to personalized ones.
- Vendor or default passwords must be changed immediately upon initial login.
- Never share passwords with anyone or accept passwords from others, especially over the phone or Internet.

7.5 Important Passwords

The Chief Technology Officer (CTO) and IT Support team hold multiple passwords necessary for accessing and managing various system components such as the firewall, applications, backup utilities, email server, and web server. The integrity and security of these passwords are critical and should be treated with the highest level of responsibility.

To ensure operational continuity, it is mandatory for the owners of these passwords to write them down on a memo, seal the memo in an envelope, and sign across all seals before securely taping the envelope shut. These sealed envelopes must then be stored in a safe under the supervision of a management member. They should only be opened as a last resort when no other viable solution exists. A record of these passwords should also be maintained to facilitate system recovery in emergency situations.

7.6 Monitoring

Company employees or consultants may occasionally receive authorization from management to test the strength of passwords used on our systems by employees. This testing may involve common cracking tools. If any weak passwords are identified during these tests, they will be disclosed exclusively to the respective employee. They will be required to change their password immediately and instructed to avoid using weak passwords in the future.

7.7 System Security

Ideally, all systems in production should automatically adhere to the password policies outlined above to minimize the risk of insecure passwords. Therefore, any systems capable of implementing these policies should have those features enabled. It is recommended to prioritize the adoption or development of software that supports these policies, particularly where it is cost-effective to do so.

8. Clean Desk & Computer Use

To enhance information security and confidentiality, the Company has implemented this policy to mitigate the risk of security breaches within the workplace. This policy aims to ensure that all information, whether in physical or digital form, is securely stored or disposed of when

workstations are unattended, and that workstations are used responsibly. For more detailed guidelines on the use of laptops and portable devices, please refer to the supplementary documents provided by the Company, which should be read alongside this policy.

The objective of this is to offer staff precise directives on storing, securing, and disposing of information to minimize the likelihood of unauthorized access, loss, or damage to information both during and outside regular business hours, especially when workstations are unattended. This policy also extends to remote workers, including those operating in public spaces or from home, where applicable.

8.1 Clean Desk Policy

Documents and reports containing sensitive or confidential information should not be left unattended on desks or in accessible areas. It is imperative to securely lock away such documentation when not under direct supervision. At the close of each day, all remaining documents should be cleared from desks and appropriately stored.

- Dispose of sensitive documents either by shredding them in designated shredder bins or by placing them in locked confidential disposal bins for later shredding.
- Whenever possible, avoid unnecessary physical storage of documents if they are already available in electronic format, except when original formats are required.
- Promptly remove printed documents from printer trays to prevent unauthorized access.
- Ensure that file cabinets containing restricted or sensitive information are kept closed and locked at all times.
- Avoid leaving access cards or keys visible on desks; store them securely when not in use.
- Refrain from jotting down personal details on sticky notes or scrap paper unless they are scheduled for same-day shredding. Never write passwords on paper.
- Erase whiteboard notes that reveal personal information immediately after use.
- Clear meeting rooms of notes written on notepads, notebooks, or any other papers after meetings.
- Embrace a paperless culture by minimizing printing and copying of documents, opting instead to retain files in electronic formats where feasible.

8.2 Equipment Use

You must respect the privacy of other users, including your colleagues, and refrain from attempting to view or read material from their monitors or devices.

- Always lock your computer if you are leaving your desk, even if just for a few minutes.
- Regularly change your password, especially if the system does not automatically enforce password changes.
- Adhere to the Password Policy & Standards.
- Properly shut down your computer, rather than switching it off directly from the power button.
- Delete unnecessary files from your personal folders and network folders to maintain organization and efficiency.

- Avoid keeping multiple electronic copies of files across different network folders.
- Do not delete electronic files belonging to colleagues or files you are uncertain about.
- Do not use a colleague's computer unless specifically authorized by your direct superior.
- Avoid storing personal data of others in your computer's personal folders.
- Refrain from using the Company's computer resources for personal profit.
- Do not make fraudulent offers of products, items, or services.
- Do not attempt to gain access to information, systems, or accounts to which you have not been assigned.

9. Portable Media and Equipment

Laptop computers, notebooks, tablets, mobile phones, and other mobile devices are essential business tools. However, their portability makes them particularly vulnerable to physical damage or theft. Additionally, since they are often used away from Company premises, they face increased threats from malicious third parties.

This section complements the computer use policy by addressing risks specific to portable computers and devices. It also applies, where relevant, to remote workers who may be working in public places or from home.

9.1 Adherence to the Policy

- Avoid leaving your device unattended and logged on. Always log off or lock it before walking away from the laptop. For mobile phones, enable a security lock mechanism such as a password, fingerprint, or pattern lock. Passwords should comply with the Company's Password Policy. This applies to personal mobile phones used to access Company data, including the Company's email.
- Keep passwords, PINs, lock patterns, tokens, and other credentials confidential. Do not share them with colleagues, friends, or third parties.
- Do not share Company laptops or devices with third parties such as family and friends.
- Store the device out of sight when not in use. Never leave a laptop, notebook, or tablet unattended in a vehicle. If necessary, you may temporarily lock it out of sight in the vehicle's trunk, but do not leave it there overnight.
- Carry and store the device in a padded bag or a strong briefcase to reduce the chance of accidental damage.
- Keep your device within your sight whenever possible. Be extra careful in public places such as airports, railway stations, or restaurants. Never leave your device unattended in public places.
- Use encryption whenever possible. If you must store files or folders locally, encrypt them; however, local storage is not encouraged. If your device is lost or stolen, encryption provides good protection against unauthorized access to data.
- When using laptops and other mobile devices, backups are normally the user's responsibility. Back up data daily by uploading it to the Company network or, if not possible, by copying it to DVD/USB devices. Encrypt backups whenever possible.

- Keep the antivirus software on your devices updated. If for any reason an update fails, inform the Company as soon as possible.

If your device is lost, stolen, damaged, or you suspect a virus/malware infection, report it to your superior immediately. This also applies to any personal devices that you have used to access or store Company data.

10. Destruction of Media and Equipment

10.1 Media Disposal

The company and its employees will adhere to the following policy:

- Shred any media, such as paper, CDs, or DVDs, that have exceeded their retention period.
- Any hard drives, USB sticks, external hard drives, tablets, digital cameras, memory cards, mobile phones, laptops, or notebooks containing Company data that no longer need to be retained will be securely wiped using an approved wiping program.
- If data tapes are used, they will be wiped with the "full erase" command via the backup software and also degaussed.
- Employees will not dispose of any media without prior approval. Approval must be requested from the CTO or the Key Compliance Officer.

10.2 Equipment Disposal

If any equipment needs to be removed from the Company's network, we will ensure that the hard drives of such equipment are thoroughly degaussed to eliminate any residual data.

Disposal of equipment will be carried out exclusively by authorized personnel. Employees are generally prohibited from disposing of any equipment.

11. Anti-Virus Protection

The term 'anti-virus software' encompasses software designed to scan for and remove various types of malware, including viruses, Trojans, worms, spyware, and adware.

The CTO, with the assistance of IT Support, will manage the antivirus and malware solutions at the Company to ensure that:

- Authorized applications and software operate in accordance with a clearly defined security policy.
- All unauthorized applications and software are prevented from being executed.

11.1 Adherence to Policy

All equipment (servers and PCs) must have valid, licensed anti-virus software installed whenever available or applicable.

- Any other hosts used by employees that are connected to the Company's Internet, Intranet, or Extranet, whether owned by the employee or the Company, must continuously run approved virus-scanning software with an up-to-date virus database, unless overridden by departmental or group policy.

- Virus definition files should be automatically updated daily.
- Anti-virus software must be set to carry out periodic scans.
- If a PC or server cannot be updated from the internet, the virus definition file should be downloaded to another machine and manually installed on the respective PC or server.
- Users must not have the option, and will not attempt, to disable or stop updates for the anti-virus software.
- If the anti-virus software is unable to clean a detected virus, users must inform the CTO to contact IT Support of the respective platform as soon as possible.
- The anti-virus software should scan every file stored on every local storage device. Incoming emails, email attachments, and external media should also be scanned.

12. Intrusion Prevention

The operation of the Company relies heavily on the availability of its technical infrastructure. System intrusions can occur through both physical unauthorized access and logical unauthorized access. To mitigate physical risks, the Company co-host its live production equipment in an ISO/IEC 27001 certified data center. This data center adheres to strict policies and procedures to ensure the security and maintenance of client equipment, allowing access only to authorized personnel.

Any system connected to the internet is at risk of attacks and compromises. Therefore, the Company's network is designed with a public interface for web server access and a private network that remains inaccessible from the internet.

The Company's policy encompasses both hardware and software components of the gaming system, as well as software on devices that remotely connect to the system. The Company will:

- Configure the firewall to allow only necessary ports, services, and internet traffic for the Company's operations.
- Permit only encrypted connections to production equipment.
- Use strong passwords for access to production equipment.
- Harden the operating system and software of the web/application server and database server by applying patches and security updates promptly.
- Implement antivirus software where applicable and regularly update virus definitions on both production equipment and machines that remotely connect to live equipment.
- Adhere to change management procedures for all changes to the production environment.
- Utilize a reputable data center for the co-location of its equipment.

13. Training

Training plays a pivotal role in information security, ensuring that employees are well-equipped to safeguard sensitive data. It comprises educating staff on policies, procedures, and best practices pertinent to information security. Training should encompass several key areas.

Firstly, general awareness training is essential for all employees, providing foundational knowledge on recognizing security threats such as phishing emails, social engineering tactics, and the significance of robust passwords. Secondly, role-specific training is crucial, tailoring instruction to individual job functions. For instance, IT personnel may require advanced training on network security measures, while HR staff should be well-versed in data protection regulations.

Thirdly, incident response training is vital, outlining protocols for reporting security breaches and guiding employees on appropriate response measures. Lastly, regular updates are imperative, ensuring continuous training to keep personnel abreast of evolving threats and advancements in technology.