**Information Technology**

**Policy Document**

**VER.6.0**

**September 2024**

**Table of Contents**

[Introduction 3](#_Toc177996518)

[Governance and Compliance 3](#_Toc177996519)

[Flintec Acceptable Use Policy 4](#_Toc177996520)

[Anti-Virus Policy 6](#_Toc177996521)

[Email Use Policy 7](#_Toc177996522)

[Information Sensitivity Policy 8](#_Toc177996523)

[Password Policy 9](#_Toc177996524)

[Removable Media Policy 11](#_Toc177996525)

[Risk Assessment Policy 13](#_Toc177996526)

[Virtual Private Network (VPN) Policy 13](#_Toc177996527)

[Wireless Communication Policy 15](#_Toc177996528)

[Backup Policy 17](#_Toc177996529)

[O365 Policy 20](#_Toc177996530)

[OneDrive Policy 20](#_Toc177996531)

[Closed Circuit Television (CCTV) Policy 21](#_Toc177996532)

[Cyber Security Policy 23](#_Toc177996533)

[Bring Your Own Device (BYOD) Policy 25](#_Toc177996534)

# Introduction

* 1. **Purpose**

This policy outlines the IT management framework for Flintec to ensure the secure, efficient, and compliant use of IT resources and services.

* 1. **Scope**

This policy applies to all employees, contractors, and third-party users who have access to IT resources and services provided by Flintec.

* 1. **Policy Objectives**

1. To ensure the security and integrity of IT resources.
2. To comply with legal and regulatory requirements.
3. To provide clear guidelines for IT resource usage and management.
   1. **Definitions**

**IT Resources**: Includes hardware, software, networks, and data.

**Users**: Employees, contractors, and third-party individuals with access to IT resources.

# Governance and Compliance

* 1. **IT Governance Framework**

The IT governance framework ensures alignment of IT strategies with business objectives and defines roles and responsibilities for IT management.

* 1. **Regulatory Compliance**

All IT practices must comply with applicable laws and regulations, including data protection and privacy laws.

* 1. **Policy Review and Update**

This policy will be reviewed annually or as needed. Updates will be communicated to all users.

# 

# Flintec Acceptable Use Policy

**1.0 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 Flintec. These systems are to be used for business purposes in serving the interests of the company, and of our clients and customers during normal operations.

Effective security is a team effort involving the participation and support of every Flintec 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.

**2.0 Purpose**

The purpose of this policy is to outline the acceptable use of computer equipment at Flintec. These rules are in place to protect the employee / employer / vendor /customer data and Flintec. Inappropriate use exposes Flintec to risks including virus attacks, cyber-attacks, data breaches, compromise of network systems and services, and legal issues.

**3.0 Scope**

This policy applies to employees, contractors, consultants, temporaries, and other workers at Flintec, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by Flintec and wherever the Flintec licensed software is used.

**4.0 Policy**

**4.1 General Use and Ownership**

1. While Flintec's network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the corporate systems remains the property of Flintec. Because of the need to protect Flintec's network, management cannot guarantee the confidentiality of information stored on any network device belonging to Flintec.
2. 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.
3. IT department of Flintec recommends that any information that users consider sensitive or vulnerable be encrypted. For security and network maintenance purposes, authorized individuals within Flintec may monitor equipment, systems and network traffic at any time.
4. Flintec reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

**4.2 Security and Proprietary Information**

1. The user interface for information contained on Internet/Intranet/Extranet-related systems should be classified as either confidential or not confidential. Examples of confidential information include but are not limited to: company private, corporate strategies, competitor sensitive, trade secrets, specifications, customer lists, and research data. Employees should take all necessary steps to prevent unauthorized access to this information.
2. Keep passwords secure and do not share accounts, except for common accounts that are strictly used for test machine operations. Authorized users are responsible for the security of their passwords and accounts. System level passwords should be changed according to the password policy guidelines on password policy.
3. All PCs, laptops, tablets, and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less, or by logging-off (control-alt-delete for Win2K users) when the host will be unattended. Flintec IT has the right to decide where this practice won’t be practical or not.
4. Use encryption of information in compliance with IT industry security standards.
5. Because information contained on portable computers is especially vulnerable, special care should be exercised.
6. Postings by employees from a Flintec email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Flintec, unless posting is in the course of business duties.
7. All hosts used by the employee that are connected to the Flintec Internet/Intranet/Extranet, whether owned by the employee or Flintec, shall be continually executing approved virus-scanning software with a current virus database unless overridden by departmental or group policy.
8. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

**4.3. Unacceptable Use**

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during 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 Flintec authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Flintec owned resources or user account.

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

* **System and Network Activities**

The following activities are strictly prohibited, with no exceptions:

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 Flintec.
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 Flintec or the end user does not have an active license is strictly prohibited.
3. 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.
4. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
5. 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.
6. Using a Flintec 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.
7. Making fraudulent offers of products, items, or services originating from any Flintec account.
8. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
9. 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.
10. Port scanning or security scanning is expressly prohibited unless prior notification to IT department is made.
11. 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.
12. Circumventing user authentication or security of any host, network or account.
13. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
14. 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.
15. Providing information about, or lists of, Flintec employees to parties outside Flintec.

* **Email and Communications Activities**

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 SMS, 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" or other "pyramid" schemes of any type.
6. Use of unsolicited email originating from within Flintec's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by Flintec or connected via Flintec's network.
7. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

# 

# Anti-Virus Policy

1. **Purpose**

To establish requirements which must be met by all computers connected to Flintec networks to ensure effective virus detection and prevention.

1. **Scope**

This policy applies to all Flintec computers that are PC-based or utilize PC-file directory sharing. This includes, but is not limited to, desktop computers, tabs, laptop computers, file/ftp/tftp/proxy servers, and any PC based equipment such as traffic generators.

1. **Policy**

All Flintec PC-based computers must have Flintec's standard, supported anti-virus software installed and scheduled to run at regular intervals. In addition, the anti-virus software and the virus pattern files must be kept up to date. Virus-infected computers must be removed from the network until they are verified as virus-free. Flintec Administrators are responsible for creating procedures that ensure anti-virus software is run at regular intervals, and computers are verified as virus-free. Any activities with the intention to create and/or distribute malicious programs into Flintec 's networks (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.) are prohibited, in accordance with the Acceptable Use Policy.

Refer to Flintec's Anti-Virus Recommended Processes to help prevent virus problems.

**Recommended processes to prevent virus problems:**

* Always run the corporate standard, supported anti-virus software.
* NEVER open any files or macros attached to an email from an unknown, suspicious, or untrustworthy source. Delete these attachments immediately, then "double delete" them by emptying your Trash.
* Delete spam, chain, and other junk email without forwarding, in with Flintec’s Acceptable Use Policy.
* Never download files from unknown or suspicious sources.
* Avoid direct disk sharing with read/write access unless there is absolutely a business requirement to do so.
* USB drives from an unknown source should be scanned for viruses before using it.
* Move all critical data to your cooperate “One Drive”.
* If software that needs to be run for the sole purpose of Flintec, conflicts with anti-virus software, run the anti-virus utility to ensure a clean machine, disable the software, and then run the desired software. After the testing is completed, enable the anti-virus software. When the anti-virus software is disabled, do not run any applications that could transfer a virus, e.g., email or file sharing.
* New viruses are discovered almost every day. Periodically check the Flintec Anti-Virus Policy and this Recommended Processes list for updates.

# Email Use Policy

1. **Purpose**

To prevent tarnishing the public image of Flintec When email goes out from Flintec to the general public will tend to view that message as an official policy statement from Flintec.

1. **Scope**

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

1. **Policy**

**3.1 Prohibited Use**

The Flintec 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 Flintec employee should report the matter to their supervisor immediately.

**3.2 Personal Use**

Using a reasonable amount of Flintec 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 Flintec email account is prohibited. Virus or other malware warnings and mass mailings from Flintec shall be approved by Flintec IT operations before sending. These restrictions also apply to the forwarding of mail received by a Flintec employee.

**3.3 Monitoring**

Flintec employees shall have no expectation of privacy in anything they store, send or receive on the company’s email system. Flintec may monitor messages without prior notice. Flintec is not obliged to monitor email messages.

# Information Sensitivity Policy

1. **Purpose**

The purpose of this Information Sensitivity Policy is to protect the confidentiality, integrity, and availability of digital information. This policy defines the classification of information based on sensitivity levels and establishes guidelines for handling, storing, and transmitting sensitive information to prevent unauthorized access, disclosure, modification, or destruction.

1. **Scope**

This policy applies to all employees, contractors, consultants, temporary staff, and other workers at Flintec, including all personnel affiliated with third parties. It covers all digital information, regardless of the medium on which it is stored, the technology used to process it, or the location from which it is accessed.

1. **Policy**

Digital information shall be classified into one of the following sensitivity levels:

1. External - Information that is intended for public disclosure. Unauthorized disclosure of this information does not pose any risk to the organization. e.g.: Press releases, marketing materials, publicly available reports.
2. Internal - Information intended for internal use within the organization. Unauthorized disclosure could have a minor impact on the organization. e.g.: Internal memos, internal emails, staff directories
3. Confidential - Information that is extremely sensitive and is restricted to a limited number of individuals. Unauthorized disclosure could have a severe impact on the organization. e.g.: Financial records, proprietary business information, internal project documents, personally identifiable information (PII), health records, trade secrets, strategic plans.

Note: Flintec personnel are encouraged to use common sense judgment in securing Flintec Confidential information to the proper extent. If an employee is uncertain of the sensitivity of a particular piece of information, he/she should contact their manager.

# Password Policy

1. **Overview**

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of Flintec’s entire corporate network. As such, all Flintec employees (including contractors and vendors with access to Flintec’s systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

1. **Purpose**

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

1. **Scope**

This policy applies to all employees, contractors, and third-party users who access Flintec systems and data

1. **Policy** 
   1. **General**

* All system-level passwords (e.g., root, enable, application administration accounts, etc.) must be changed on at least three months basis (90 days).
* All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every three months (90 days).
* Passwords must not be inserted into email messages or other forms of electronic communication.
* All user-level and system-level passwords must conform to the guidelines described below.
  1. **Guidelines**

**A. General Password Construction Guidelines**

1. Length: Minimum of 12 characters.
2. Complexity: Passwords must include:

- At least one uppercase letter (A-Z)

- At least one lowercase letter (a-z)

- At least one digit (0-9)

- At least one special character (e.g., !, @, #, $, %, ^, &, \*)

Poor, weak passwords have the following characteristics:

* Avoid using easily guessable passwords such as "password", "123456", "qwerty", etc.
* Do not use personal information (e.g., names, birthdays) in passwords.
* Do not reuse passwords across multiple accounts.

**B. Password Usage**

1. Unique Passwords: Use different passwords for different systems and accounts.
2. Password Sharing: Do not share passwords with anyone. If a password must be shared for business purposes, use a secure method and change the password immediately after.
3. Password Storage: Do not write down passwords or store them in plain text files. Use a secure password manager if necessary.
4. Secure Password Entry: Be aware of your surroundings when entering your password to avoid shoulder surfing.

**Note:** If someone demands a password, refer them to this document or have them call someone in the IT Department

**C. Password Change**

1. Frequency: Change passwords at least every 90 days.
2. Forced Change: Change passwords immediately if there is suspicion or evidence of compromise.
3. Password History: Users cannot reuse their last 5 passwords.

**D. Account Lockout**

1. Failed Attempts: After 5 unsuccessful login attempts, the account will be locked for 30 minutes.
2. Unlocking Accounts: Contact IT support to unlock an account before the 30-minute lockout period if necessary

**E. Multi-Factor Authentication (MFA)**

1. Requirement: Enable MFA on all accounts where possible to provide an additional layer of security.
2. Methods: Acceptable MFA methods include:

- Authenticator apps (e.g., Microsoft authenticator app)

- SMS (where authenticator apps are not feasible)

- Hardware tokens

**F. Responsibilities**

All users should:

1. Create and maintain strong passwords.
2. Keep passwords confidential.
3. Report any suspected password compromise immediately.

**G. Compliance**

Non-compliance with this policy may result in disciplinary action, up to and including termination of employment or contract.

# Removable Media Policy

**1.0 Overview**

Removable media is a well-known source of malware infections and has been directly tied to the loss of sensitive information in many organizations.

**2.0 Purpose**

The purpose of this policy is to outline the guidelines and requirements for the use of removable media within the Flintec to ensure the security and integrity of the organization's data and information systems. Removable media include, but are not limited to, USB drives, external hard drives, CDs, DVDs, and other portable storage devices.

**3.0 Scope**

This policy applies to all employees, contractors, temporary workers, and other personnel who use removable media in conjunction with the Flintec’s computer systems, networks, or data.

**4.0 Policy**

* 1. **General Use**

1. Authorization Employees must obtain authorization from their department manager or IT department before using removable media on any organization-owned device.
2. Approved Devices: Only removable media devices approved by the IT department are allowed for use within the organization. Unauthorized devices are **strictly prohibited**.
3. Data Encryption: All sensitive or confidential data stored on removable media must be encrypted using encryption methods approved by the IT department.
4. Scanning for Malware: All removable media must be scanned for malware and viruses by the organization's approved antivirus software before being connected to any organizational device.
5. Data Transfer: Employees must ensure that only the minimum necessary amount of sensitive data is transferred to removable media and that this data transfer is documented, including the type of data and the reason for its transfer.
6. Reporting Loss or Theft: Any loss or theft of removable media containing organizational data must be reported immediately to the IT department and the employee's direct supervisor.

**4.2 Usage Restrictions**

1. Personal Use: The use of removable media for personal purposes is strictly prohibited on all organizational devices.
2. Unapproved Software: Installing or running software directly from removable media without prior approval from the IT department is prohibited.
3. External Devices: Removable media obtained from untrusted sources (e.g., found devices or borrowed from non-employees) must not be used with organizational systems.
4. Storage of Sensitive Information: Removable media should not be used to store sensitive information long-term. Data should be transferred to a secure location as soon as possible.
5. Physical Security: Users must ensure that removable media devices are always kept secure. When not in use, removable media should be stored in a secure location.

**4.3 Disposal of Removable Media**

1. Data Wiping: Before disposal, all data on removable media must be securely erased using methods approved by the IT department to prevent data recovery.
2. Physical Destruction: Removable media that is no longer needed and cannot be securely erased should be physically destroyed to prevent unauthorized access to data.

**5.0 Enforcement**

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. Contractors, temporary workers, and other personnel may have their access to organizational systems and data revoked.

**6.0 Exceptions**

Exceptions to this policy may be granted on a case-by-case basis, and must be approved in writing by the IT Department.

**7.0 Definitions**

Removable Media: Any portable device or media used for data storage, including USB flash drives, external hard drives, CDs, DVDs, memory cards, and other portable devices.

Sensitive Data: Any information that, if lost, stolen, or improperly disclosed, could result in financial loss, damage to reputation, or legal consequences for the organization.

# Risk Assessment Policy

1. **Purpose**

To empower IT department to perform periodic information security risk assessments (RAs) for the purpose of determining areas of vulnerability, and to initiate appropriate remediation.

1. **Scope**

Risk assessments can be conducted on any entity within Flintec or any outside entity that has signed a Third-Party Agreement with Flintec. RAs can be conducted on any information system, to include applications, servers, and networks, and any process or procedure by which these systems are administered and/or maintained.

1. **Policy**

The execution, development and implementation of remediation programs are the joint responsibility of Flintec IT Department and the departments responsible for the systems are being assessed. Employees are expected to cooperate fully with any RA being conducted on systems for which they are held accountable. Employees are further expected to work with the IT department Team in the development of a remediation plan.

1. **Definitions**

Entity Any business unit, department, group, or third party, internal or external to Flintec, responsible for maintaining Flintec assets.

Risk Those factors that could affect confidentiality, availability, and integrity of Flintec’s key information assets and systems. Flintec is responsible for ensuring the integrity, confidentiality, and availability of critical information and computing assets, while minimizing the impact of security procedures and policies upon business productive

# Virtual Private Network (VPN) Policy

1. **Purpose**

The purpose of this policy is to define the requirements and guidelines for using Virtual Private Networks (VPNs) to access the organization's network remotely. This policy aims to protect the security and integrity of the organization's network and data while allowing employees and authorized personnel to perform their duties effectively from remote locations.

1. **Scope**

This policy applies to all employees, contractors, consultants, temporary staff, and other authorized users who use a VPN to access the organization's network, applications, and data remotely. It covers all VPN connections used to access the organization's resources, regardless of device or location.

1. **Policy**

**3.1 Authorized Use**

1. Access Authorization: VPN access is granted only to employees and authorized personnel who require remote access to the organization's network to perform their job duties. Access must be requested and approved by the user's manager and the IT department.
2. Approved Devices: Only organization-approved devices with up-to-date security software and configurations are permitted to connect to the VPN. Personal devices may not be used for VPN access unless explicitly approved by the IT department.
3. Network Access: VPN users are only allowed access to the network resources necessary for their job function. Access to sensitive or restricted resources must be authorized by the appropriate department head or data owner.
4. VPN Client Software: Users must use the organization's standard VPN client software, configured according to IT department guidelines. The use of unapproved VPN software is prohibited.

**3.2 Security Requirements**

1. Encryption: All VPN connections must use strong encryption methods, as defined by the IT department, to ensure data transmitted over the VPN is secure.
2. Multi-Factor Authentication (MFA): All VPN connections must use multi-factor authentication (MFA) to verify the user's identity before granting access to the organization's network where possible.
3. Password Protection: Users must follow the organization's password policy when creating and managing their VPN login credentials. Sharing of VPN credentials is strictly prohibited.
4. Software Updates: All devices used for VPN access must have up-to-date operating systems, security patches, and antivirus software to minimize the risk of malware and other security threats.
5. Session Timeout: VPN sessions must automatically disconnect after a 30 mins period of inactivity, as determined by the IT department, to reduce the risk of unauthorized access.

**3.3 User Responsibilities**

1. Connection Integrity: Users are responsible for maintaining the security and confidentiality of their VPN connections. This includes ensuring their devices are secure, passwords are protected, and no unauthorized users have access to their devices or VPN sessions.
2. Reporting Incidents: Any suspected security incidents, including potential unauthorized access or loss of devices used for VPN access, must be reported immediately to the IT department.
3. Data Handling: Users must follow the organization's data handling and classification policies when accessing or transmitting data over the VPN. Sensitive or confidential information should be handled with appropriate security measures.

**4.0. Compliance**

Failure to comply with this policy may result in disciplinary action, up to and including termination of employment. Contractors, consultants, and temporary staff may have their access to the organization's network and resources revoked.

**5.0 Exceptions**

Any exceptions to this policy must be documented and approved by the IT department and the General Manager IT (GM IT).

**6.0 Definitions**

Virtual Private Network (VPN): A technology that creates a secure, encrypted connection over a less secure network, such as the internet, allowing remote users to securely access the organization's internal network.

Remote Access: The ability to access the organization's network and resources from a location outside the organization's physical premises, using a VPN or other secure connection methods.

Multi-Factor Authentication (MFA): A security system that requires more than one method of authentication to verify the user's identity for a login or other transaction.

# Wireless Communication Policy

**1.0 Purpose**

The purpose of this policy is to establish guidelines for the secure use of wireless communication technologies within the organization. This policy aims to protect the organization’s information assets and network infrastructure from potential security threats associated with wireless communication.

**2.0 Scope**

This policy applies to all employees, contractors, temporary staff, and other personnel who use wireless communication devices, including but not limited to wireless laptops, smartphones, tablets, and other devices capable of wireless communication, to access the organization's network or resources. It also applies to all wireless access points and infrastructure devices used within the organization's premises.

**3.0 Policy**

**3.1 Wireless Network Access**

1. Authorized Devices: Only devices authorized and configured by the IT department are permitted to connect to the organization's wireless network. Personal devices must not be connected to the organization's internal wireless network unless explicitly authorized for business purposes.
2. Network Segmentation: The organization’s wireless network must be segmented from the wired network using appropriate security measures, such as firewalls and access control lists (ACLs), to limit access to sensitive information and resources.
3. SSID Management: The organization's wireless networks must use non-identifiable SSIDs (i.e., names that do not reveal the organization’s identity or purpose) to reduce the risk of targeted attacks. Broadcasting of the SSID may be disabled unless necessary for business operations.
4. Guest Access: A separate guest wireless network must be provided for visitors, contractors, and other non-employees. The guest network must be isolated from the organization’s internal network and provide limited internet access with strong security controls.

**3.2 Security Requirements**

* 1. Encryption Standards: All wireless networks must use strong encryption protocols, such as WPA3 or the most current industry-standard encryption, to protect data transmitted over the network. WEP and WPA are not permitted.
  2. Authentication: Access to the organization's wireless network must require authentication using methods approved by the IT department, such as WPA2/WPA3-Enterprise, which requires a username and password or digital certificates.
  3. Device Configuration: All wireless devices connecting to the organization's network must be configured to adhere to the organization's security policies, including having updated antivirus software, firewalls, and security patches.
  4. MAC Address Filtering: The organization may implement MAC address filtering to restrict network access to approved devices only. This control should be managed and regularly updated by the IT department.

**3.3 User Responsibilities**

1. Securing Devices: Users are responsible for ensuring their wireless devices are secure and compliant with the organization's policies. This includes applying updates, using encryption, and avoiding the use of open or unsecured wireless networks for business activities.
2. Reporting Security Incidents: Any suspected security incidents, including unauthorized access to the wireless network or loss of a device used to access the network, must be reported immediately to the IT department.
3. Avoiding Rogue Access Points: Users must not connect to unauthorized wireless access points or create personal hotspots that could bypass the organization’s network security controls.

**3.4 Wireless Infrastructure Management**

1. Installation of Access Points: Only the IT department is authorized to install or modify wireless access points and related infrastructure. Unauthorized installation of wireless devices is strictly prohibited.
2. Regular Audits: The IT department must perform regular audits of the wireless network to detect and remove unauthorized devices, ensure compliance with security policies, and identify any potential vulnerabilities.
3. Firmware Updates: All wireless infrastructure devices, including access points and controllers, must have their firmware regularly updated to the latest stable versions to protect against known vulnerabilities.

**4.0. Compliance**

Failure to comply with this policy may result in disciplinary action, up to and including termination of employment. Contractors, consultants, and temporary staff may have their access to the organization's network and resources revoked.

**5.0 Exceptions**

Any exceptions to this policy must be documented and approved by the IT department and the General manager IT (GM IT).

**6.0 Definitions**

**Wireless Communication:** The transmission of data or voice signals without the use of physical connections, typically using radio frequencies, including Wi-Fi, Bluetooth, and cellular networks.

**Access Point (AP)**: A device that allows wireless devices to connect to a wired network using Wi-Fi or other wireless standards.

**SSID (Service Set Identifier):** The name assigned to a wireless network to identify it to users and devices.

**Encryption**: The process of converting data into a code to prevent unauthorized access.

# Backup Policy

1. **Purpose**

The purpose of this policy is to define the requirements for data backup and recovery to protect the organization's information assets and ensure business continuity. This policy aims to minimize data loss and ensure the ability to recover data and systems in the event of accidental deletion, hardware failure, cybersecurity incidents, or other disruptions.

1. **Scope**

This policy applies to all organizational units, employees, contractors, and third-party vendors who are responsible for managing or using the organization’s information systems and data. It covers all data and systems deemed critical to the operation of the organization, including servers, databases, applications, and user workstations

**3.0 Policy**

**3.1 On-Site Backup** - The organization will maintain on-site backups for all critical data, applications, and systems. On-site backups will be stored on secure, dedicated backup servers located within the primary data center or office. These backups will be conducted daily, and the data will be encrypted and protected with access controls. On-site backups are intended for rapid recovery of data in the event of localized incidents or data corruption

**3.2 Off-Site Backup -** The organization will also implement off-site backups to provide additional protection against data loss due to physical disasters, theft, or other catastrophic events. Off-site backups will be conducted at least weekly, with full backups replicated to a secure remote location or cloud storage provider. These backups will be encrypted both in transit and at rest, and access will be restricted to authorized personnel only. Off-site backups are a critical component of the organization’s disaster recovery plan, ensuring data availability even if the primary site is compromised.

**3.3 Timing**

Backups are made according to the Backup schedule table. This table should be updated according to the current requirement of the enterprise.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **Daily** | | | | | **Weekly** | | | | | | **Monthly** | | | | | | **Yearley** | | | | |
| **System Name** | **Backup** | **Retention Period** | **Tape** | **Offsite** | **Cloude** | **Backup** | **Retention Period** | **Tape** | **Offsite** | **Cloude** | **Backup** | | **Retention Period** | **Tape** | **Offsite** | **Cloude** | **Backup** | | **Retention Period** | **Tape** | **Offsite** | **Cloude** |
| **ERP** | No | N/A |  |  |  | Full | 14 Days | X |  | X | Full | | 12 Months | X |  | X | Full | | 5 Years | X |  | X |
| **HR & Time attendance** | No | N/A |  |  |  | Full | 14 Days | X | X | X | Full | | 12 Months | X | X | X | Full | | 5 Years | X | X | X |
| **Active Directory** | No | N/A |  |  |  | Full | 14 Days |  |  |  | No | | N/A |  |  |  | No | | N/A |  |  |  |
| **PDM SQL** | Full | 14 Days | X | X | X | No | N/A |  |  |  | Full | | 12 Months | X | X |  | Full | | 1 Year | X | X |  |
| **PDM** | Full | 14 Days | X |  |  | No | N/A |  |  |  | Full | | 12 Months | X |  |  | Full | | 1 Year | X |  |  |
| **Production Automation System** | Full | 14 Days | X | X | X | No | N/A |  |  |  | No | | N/A |  |  |  | Full | | 1 Year | X | X | X |
| **Attendance Data** | No | N/A |  |  |  | Full | 14 Days | X | X | X | No | | N/A |  |  |  | No | | N/A |  |  |  |

**3.4 Tape / Mass Storage**

There shall be a separate set of tapes or mass storage device for each backup day including Monday to Friday.

**3.5 Tape Drive Cleaning**

Tape drives shall be cleaned weekly, and the cleaning tape shall be changed monthly.

**3.6 Age of tapes**

The date each tape was put into service shall be recorded on the tape. Tapes that have been used longer than one year shall be discarded and replaced with new tapes.

**3.7 Responsibility**

The IT Manager shall delegate a member of the IT department to perform regular backups. The delegated person shall develop a procedure for testing backups and test the ability to restore data from backups monthly.

**3.8 Testing**

The ability to restore data from backups shall be tested at least once per month.

**3.9 Restoration**

In a failure the last successful backup will be restored and if there is a time gap between the backup and the failure, the data needs to be entered manually.

Users should keep their data on OneDrive. Refer OneDrive policy for more information.

**3.10 Tape / Mass Storage Locations**

Offline tapes or mass storage devices used for nightly backup shall be stored off-site. Monthly tapes shall be stored in a fireproof safe.

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

* 1. **Definitions**

**Backup** - The saving of files onto magnetic tape or other offline mass storage media for the purpose of preventing loss of data in the event of equipment failure or destruction.

**Archive** - The saving of old or unused files onto magnetic tape or other offline mass storage media for the purpose of releasing on-line storage room.

**Restore** - The process of bringing offline storage data back from the offline media and putting it on an online storage system such as a file server.

# O365 Policy

**1.0 Overview**

Microsoft O365 solutions are the new trend of Cloud computing technologies that are available on the market that an organization can subscribe.

**2.0 Purpose**

This policy defines the acceptable use, security, and management guidelines for OneDrive for Business within Flintec. It aims to ensure that OneDrive is used efficiently, securely, and in compliance with organizational and regulatory requirements.

.

**3.0 Scope**

This policy covers all users that has an Flintec corporate O365 account and that includes but not limited to Flintec employees, contractors, consultants, temporaries, and other workers including all personnel affiliated.

**4.0 Policy**

Users are authorized to use their O365 accounts and install office on any 5 devises. The no of devises may vary depending on the declaration made by Microsoft.

All devises that are additionally installed with the Flintec account, should comply with the Flintec Anti-Virus policy to minimize the risk of corporate network affecting with virus.

Users are advised not to save their O365 password on any device. Saving the password increases the risk of data breaches and if such situations occur, the user will be liable to pay any financial losses and legal fees.

All conditions of the e mail policy will be applicable for O365 users

**5.0 Definitions**

O365 - Office 365 is the brand name Microsoft uses for a group of subscriptions that provides productivity software and a related service

Employees who violate this policy will be subject to disciplinary action, up to and including termination of employment.

# OneDrive Policy

1. **Overview**

Microsoft OneDrive is an online cloud storage service from Microsoft that allows the user, with an O365 corporate license, use of 1TB of Cloud storage.

1. **Purpose**

This policy defines the acceptable use, security, and management guidelines for OneDrive for Business within Flintec. It aims to ensure that OneDrive is used efficiently, securely, and in compliance with organizational and regulatory requirements.

**3.0 Scope**

This policy covers all users that has been authorized to have and to use a Flintec corporate O365 account. This includes, but not limited to, Flintec employees, contractors, consultants, temporaries, and other workers including all personnel affiliated.

**4.0 Policy**

All data should be stored on the Flintec corporate OneDrive and no data should be stored out of the local OneDrive folder.  For speedy and offline access, OneDrive could be synchronized with the local PC to create a cached copy of the data. By default, sharing data is limited to Flintec users and if external sharing is required, it should be authorized by a senior manager.

All devices that are using the corporate OneDrive, should comply with the Flintec Anti-Virus policy to minimize the risk of the corporate network being affected with a virus.

Users are advised not to save their O365 password on any device. Saving the password increases the risk of data breaches and if such a situation occurs, the user will be liable to pay any financial losses and legal fees.

# Closed Circuit Television (CCTV) Policy

1. **Purpose**

The Closed-Circuit Television (CCTV) Policy establishes the principles and operational procedures for the installation and use of CCTV by Flintec.

1. **Scope**

Flintec is committed to providing a safe and secure working environment. Where necessary and appropriate Flintec will use CCTVs to protect people and assets in and around Flintec property, while also respecting and protecting the individual's right to privacy. The use of CCTV is part of an integrated security approach that includes several strategies, including access controls, lighting, alarms and security staff.

**3.0 Policy**

Flintec have an obligation to ensure the working environment is safe and secure and fulfil duty of care to employees and visitors. The CCTV system exists to assist Flintec to fulfil these obligations and to prevent and manage other inappropriate behavior in Flintec. CCTV provides enhanced capability to protect Flintec’s assets against vandalism and theft. The presence of CCTV cameras discourages misconduct and inappropriate behavior and assures staff and visitors that they are protected when on Flintec. This policy describes how our CCTV system does this.

**Use of CCTV**

* Prevent and verify incidents involving
* Criminal behavior
* Internal accidents
* Staff misconduct
* Staff work performance
* To provide the security staff with visual coverage during emergencies

**CCTV cameras are NOT**:

* Hidden
* Located in private areas such as toilets, changing rooms

**Access to CCTV footage**

CCTV footage is only accessed for the purposes set out in this policy and only by the following people:

* 1. All senior managers
  2. People explicitly authorized by senior managers

3. Any other people permitted by law.

**Showing footage to staff involved in incidents**

When using CCTV for the purposes listed in this policy under the heading ‘Use of CCTV’ and only when appropriate, the HR / IT may show specific footage of an incident to those directly involved, including relevant staff upon formal request made by HR or senior manager.

This means that any person on Flintec premises may be captured on CCTV footage of an incident that the HR / IT may subsequently show to staff.

Flintec cannot give copies of CCTV footage to staff.

Any requests for a copy of CCTV footage must be made to the HR Department.

**Managing and securing the CCTV system**

The IT Manager or their nominee is responsible for managing and securing the CCTV system including:

1. Operation of the CCTV system and ensuring it complies with this policy

2. Considering the appropriate location and use of cameras and method for storing CCTV footage

3. Maintaining and upgrading cameras when required.

**Disclosure of CCTV footage**

Flintec may only disclose CCTV footage externally as described in this policy or otherwise when permitted by law.

**Storage of Footage**

CCTV footage is kept for no more than 31 days. If Flintec has not used CCTV footage in any of the ways set out above, and there has been no request to view or access footage during this period, the footage is deleted.

Where CCTV footage has been used to verify an incident or where it is required to be retained for legal reasons, HR will manage and securely retain the footage in accordance with the above.

# Cyber Security Policy

**1.0 Purpose**

The purpose of this Cyber Security Policy is to establish a comprehensive framework to protect Flintec’s assets, information systems, and data from cyber threats, ensuring confidentiality, integrity, and availability.

**2.0 Scope**

This policy applies to all employees, contractors, vendors, and third parties who have access to the company's networks, systems, applications, and data.

**3.0 Policy**

3.1 Governance and Responsibilities

3.1.1 Management

1. Flintec Management will provide leadership, support, and resources necessary to implement and maintain effective cyber security measures.
2. General Manger IT Manager and the System Engineers / System Administrators will be responsible for overseeing the implementation, enforcement, and review of this policy.

3.1.2 Employees

1. All employees must comply with this policy and support the company's efforts to maintain a secure computing environment.
2. Employees should receive regular training and education on cyber security awareness, policies, and best practices.

3.2 Risk Management

1. Conduct regular risk assessments to identify potential threats, vulnerabilities, and the potential impact on the organization.
2. Develop and maintain a risk management framework to prioritize and address identified risks effectively.
3. Implement appropriate controls to mitigate and manage risks based on industry best practices and regulatory requirements.

3.3 Access Control

1. Enforce strong access control mechanisms, granting access privileges based on the principle of least privilege.
2. Use strong passwords or passphrase policies, enforce regular password changes, and implement multi-factor authentication (MFA) for critical systems and accounts. Refer Flintec password policy.
3. Implement user account management practices, such as timely revocation of access upon termination or change in job roles.

3.4 Data Protection and Privacy

1. Classify data based on its sensitivity and criticality and implement appropriate security controls for each category.
2. Encrypt sensitive data at rest and in transit using industry-standard encryption algorithms.
3. Regularly backup data and test restoration procedures to ensure availability and integrity.
4. Adhere to applicable data protection and privacy regulations, including data handling, retention, and disclosure requirements.

3.5 Network Security

1. Implement robust network perimeter security measures, including firewalls, intrusion detection and prevention systems (IDPS), and secure configurations.
2. Secure wireless networks using encryption, strong authentication mechanisms, and regular monitoring.
3. Segment networks to minimize the impact of potential breaches and implement strong network monitoring and logging capabilities.

3.6 Malware Protection

1. Deploy up-to-date antivirus software on all endpoints, servers, and gateways.
2. Regularly update operating systems, applications, and firmware to address vulnerabilities promptly.
3. Educate employees about the risks of malware, phishing, and social engineering attacks, and provide guidelines for safe computing practices.

3.7 Incident Response and Recovery

1. Develop an incident response plan outlining roles, responsibilities, and procedures to detect, respond to, and recover from security incidents. Refer IT Contingency Management Plan
2. Establish a dedicated incident response team or designate responsible individuals to handle security incidents.
3. Conduct regular incident response drills and post-incident reviews to continuously improve response capabilities.

3.8 Vendor and Third-Party Management

1. Assess the security practices and controls of third-party vendors before engaging in business relationships.
2. Implement appropriate contractual agreements addressing security requirements, incident reporting, and data protection.
3. Regularly monitor and review the security practices of vendors to ensure ongoing compliance.

3.9 Physical Security

1. Implement physical security measures to protect critical infrastructure, data centers, and sensitive areas.
2. Control and monitor physical access to premises, server rooms, and equipment.
3. Properly dispose of sensitive information and electronic devices to prevent unauthorized access or data leakage.

3.10. Awareness and Training

1. Regularly educate employees about cyber security risks, policies, and best practices.
2. Conduct periodic training sessions, workshops, and awareness campaigns to promote a security-conscious culture.

3.11. Compliance and Audit

1. Regularly conduct internal audits and assessments to evaluate compliance with this policy and relevant regulations.
2. Monitor and analyze security logs, conduct periodic vulnerability assessments, and penetration tests to identify weaknesses and address them promptly.
3. Report and remediate any identified non-compliance issues promptly.

3.12 Policy Review

This policy will be reviewed at least annually or whenever there are significant changes to the organization's technology, infrastructure, or cyber threat landscape.

By implementing this Strong Cyber Security Policy, our company demonstrates its commitment to protecting sensitive information, maintaining operational resilience, and safeguarding the trust of our clients, employees, and partners.

# Bring Your Own Device (BYOD) Policy

1. **Purpose**

The purpose of this policy is to outline the guidelines and procedures for employees who use personal devices to access organizational resources. The aim is to ensure the security, integrity, and appropriate use of Flintec’s data and IT systems while allowing employees to use their personal devices for work purposes.

**2.0 Scope**

This policy applies to all employees, contractors, and third-party users who use personal devices (e.g., smartphones, tablets, laptops) to access organizational resources, including email, applications, and data.

**3.0 Device Registration and Approval**

3.1 Device Registration

Employees must register their personal devices with the IT department before accessing organizational resources. Registration includes providing device details and installing necessary security software as required by the IT department.

3.2 Device Approval

All devices must be approved by the IT department to ensure they meet security standards. The IT department will review and approve devices based on security criteria and organizational requirements.

**4.0 Security Requirements**

4.1 Security Software

Personal devices must have up-to-date security software installed, including antivirus and anti-malware tools. Employees are responsible for keeping their security software current.

4.2 Password Protection

Devices must be protected with a strong password or biometric authentication. Passwords must adhere to the organization’s password policy, including complexity and change requirements.

4.3 Encryption

Devices must be encrypted to protect organizational data stored on them. Full-disk encryption or similar measures must be enabled.

4.4 Security Patches and Updates

Employees must regularly apply security patches and updates to their devices. The IT department may provide guidance on necessary updates.

**5.0 Access and Use**

5.1 Access Controls

Access to organizational resources must be secured through VPNs, multi-factor authentication (MFA), or other approved methods. Access will be granted based on job roles and necessity.

5.2 Data Access and Storage

Employees must use secure methods for accessing and storing organizational data. Data should be accessed through approved applications and not stored locally unless necessary and authorized.

5.3 Application Management

Only approved applications may be used to access organizational resources. Employees must ensure that applications used for work purposes comply with security and privacy standards.

**6.0 Privacy and Data Protection**

6.1 Personal and Organizational Data Separation

Employees must separate personal data from organizational data on their devices. Organizational data should be stored in designated areas and not mixed with personal information.

6.2 Data Privacy

The organization’s data privacy policies apply to any data accessed or stored on personal devices. Employees must handle organizational data with the same level of confidentiality and care as if using company-owned devices.

**7.0 Lost or Stolen Devices**

7.1 Reporting

Employees must immediately report lost or stolen devices to the IT department. Prompt reporting helps mitigate potential security risks.

7.2 Remote Wipe

The IT department may remotely wipe organizational data from lost or stolen devices to protect sensitive information. This action will be taken following the organization’s incident response procedures.

**8.0 Compliance and Monitoring**

8.1 Policy Compliance

Employees must comply with all aspects of this BYOD policy. Non-compliance may result in disciplinary action, including the revocation of BYOD privileges.

8.2 Monitoring

The IT department may monitor devices for compliance with this policy and to ensure the security of organizational data. Monitoring will be conducted in accordance with applicable laws and regulations.

**9.0 Support and Maintenance**

9.1 IT Support

The IT department will provide support for issues related to accessing organizational resources on personal devices. Support will be limited to connectivity and security issues and does not cover general device troubleshooting.

9.2 Device Maintenance

Employees are responsible for maintaining their devices, including hardware and software. The IT department will not provide repair or replacement services for personal devices.

**10.0 Termination of Employment or BYOD Enrollment**

10.1 Device Removal

Upon termination of employment or removal from the BYOD program, employees must remove organizational data and applications from their personal devices. The IT department will provide instructions for data removal.

10.2 Revocation of Access

Access to organizational resources from personal devices will be revoked as part of the offboarding process. The IT department will ensure that all access rights are removed.

**11.0 Policy Review and Updates**

11.1 Review

This policy will be reviewed annually or as needed to ensure it remains current and effective. Updates will be communicated to all users.

11.2 Updates

Any changes to this policy will be distributed to all employees, and updated versions will be made available through the organization’s internal communication channels.