

Policy Title: Internet Access Policy

Effective Date: [25th Aug 2025]

An **Internet Access Policy** is a set of guidelines established by an organization to govern the use of the internet and associated online resources by its employees and office staff. These policies aim to ensure that internet access is used responsibly, securely, and in accordance with the organization's goals and legal requirements.

Here's an overview of what an Internet Access Policy might include:

1. Purpose and Scope

- **Purpose:** To outline the acceptable use of internet resources to ensure productivity, security, and compliance with legal regulations.
- **Scope:** Specifies the employees, departments, or systems covered by the policy, such as all users accessing the company's network or only certain roles (e.g., IT staff, office Senior Staff).

2. Acceptable Use

- **Business Use:** Internet access should primarily be used for work-related tasks (research, communication, information, etc.).
- **Personal Use:** Limited personal use may be allowed but should not interfere with work or consume excessive bandwidth.
- **Prohibited Activities by Firewall Device**
 - Accessing illegal, harmful, or inappropriate content (e.g., pornography, hate speech, etc.).
 - Engaging in illegal activities (e.g., hacking, piracy, downloading unauthorized software).
 - Cyberbullying, harassment, or any behavior that violates the organization's code of conduct.
 - Excessive personal use or time-wasting activities (e.g., excessive social media browsing, online gaming, etc.).

3. Security and Privacy

- **Data Protection:** Users should not share sensitive company data over unsecure channels (e.g., public Wi-Fi, unsecured websites).
- **Malware and Threats:** Employees should avoid downloading suspicious files, clicking on unknown links, or engaging in activities that could introduce malware or other security threats.
- **Monitoring:** The organization may monitor internet activity for compliance, performance analysis, and security purposes. Employees should be aware that their online activities could be subject to monitoring.

4. Access Controls

- **Login Credentials:** Employees must use secure, unique login credentials for accessing company systems and networks.
- **Access Restrictions:** Certain websites or services may be blocked or restricted (e.g., social media, gambling sites, or streaming services).
- **Remote Access:** Guidelines for accessing the company network from remote locations (e.g., using VPNs, two-factor authentication).

5. Compliance with Laws and Regulations

- **Copyright Laws:** Employees should adhere to copyright laws and avoid unauthorized sharing of intellectual property.
- **Data Compliance:** Employees should comply with data protection laws (e.g., GDPR, CCPA) when using the internet for work-related purposes.
- **Monitoring and Auditing:** The company may conduct audits and maintain logs of internet activity to ensure compliance with this policy.

6. Consequences of Violation

- **Disciplinary Actions:** Consequences for violating the policy could include disciplinary measures ranging from warnings to termination, depending on the severity of the breach.
- **Legal Actions:** In cases of illegal activity, the organization may report violations to law enforcement or pursue legal action.

7. Review and Updates

- The policy should be reviewed periodically to ensure it remains up to date with new technologies, legal requirements, and organizational needs.
- **Use for Work Purposes**
 - Access the internet mainly for work-related tasks.
 - Keep personal use minimal and non-disruptive.
- **Avoid Harmful or Illegal Content**
 - Do not visit or download from suspicious or inappropriate websites (e.g., adult, gambling, pirated software).
 - Never engage in illegal online activities (e.g., hacking, torrenting, data theft).
- **Protect Company Data**
 - Do not share confidential or sensitive information online without proper authorization.
 - Use encrypted channels (HTTPS, VPN) when transmitting sensitive data.
- **Beware of Malware and Phishing**
 - Avoid clicking on unknown links or downloading unverified attachments.
 - Report suspicious emails or websites to IT immediately.

Follow Security Protocols

- Use strong, unique passwords and enable two-factor authentication.
- Lock your screen and log out when stepping away.

•Respect Monitoring Policies

- Internet use may be monitored. Avoid any behavior you wouldn't want reviewed.
- Do not try to bypass security filters or restrictions.

• Comply with Laws and Company Rules

- Follow copyright laws and data protection regulations (e.g., GDPR, HIPAA).
- Stay updated with any changes to company internet use policy.

• Consequences for Violations

- VT Capital fined any type of violating this policy can lead to disciplinary action, including termination or legal action.

Policy Title: Risk Parameter Controls Policy

Effective Date: [25th Aug 2025]

1. Purpose The purpose of this policy is to outline the controls and procedures necessary to manage and mitigate risk parameters within **VT Capital Market Pvt Ltd**. This policy aims to establish a framework for identifying, monitoring, and controlling various risk parameters, ensuring the Company operates in a prudent and compliant manner.

2. Scope this policy applies to all employees, stakeholders, and relevant parties involved in the operations and decision-making processes of VT Capital Market Pvt Ltd.

3. Definitions

- a. Risk Parameters: The measurable factors that define and quantify various risks associated with the Company's activities, including but not limited to market risk, credit risk, liquidity risk, operational risk, and legal and regulatory risk.
- b. Controls: The mechanisms, processes, and procedures designed to identify, assess, monitor, and Mitigate risks.

4. Risk Parameter Controls

a. Identification of Risk Parameters

- i) The Company shall identify and define key risk parameters applicable to its business Operations.
- ii) Risk parameters may include, but are not limited to: - Market risk indicators (e.g., volatility, Liquidity, concentration) - Credit risk indicators (e.g., credit ratings, counterparty exposure) - Liquidity risk indicators (e.g., funding sources, cash flow projections) - Operational risk Indicators(e.g., system failures, internal fraud) - Legal and regulatory risk indicators (e.g., Compliance with laws, regulatory changes).

b. **Risk Measurement and Monitoring**

- i) The Company shall establish robust systems and processes to measure and monitor risk Parameters.
- ii) Regular risk assessments shall be conducted to evaluate the impact and probability of risks.
- iii) The monitoring process should include timely and accurate risk reporting to senior Management and relevant stakeholders.
- iv) Key risk indicators shall be set, and tolerance limits established for each risk parameter.
- v) Deviations from established risk parameters and tolerance limits should trigger appropriate actions, including escalation to senior management.

c. **Risk Mitigation and Controls**

- i) The Company shall implement appropriate risk mitigation strategies and controls for each identified risk parameter.
- ii) Mitigation measures may include diversification of investments, hedging strategies, stress testing, and the establishment of contingency plans.
- iii) Regular review and enhancement of risk controls should be conducted to address emerging risks and changes in the business environment.
- iv. Risk controls should be documented, communicated, and implemented consistently across the Organization.
- v. Responsible individuals or teams should be designated for the oversight and implementation of Risk controls.

d. **Compliance and Regulatory Requirements**

- i) The Company shall ensure that risk parameter controls are in compliance with applicable laws, Regulations, and industry best practices.
- ii) Compliance with regulatory requirements and reporting obligations related to risk parameters Should be given utmost priority.
- iii) Regular internal and external audits shall be conducted to assess the effectiveness of risk Parameter controls and ensure compliance.

- 5. **Training and Awareness** The Company shall provide regular training and awareness programs to employees and relevant stakeholders on risk parameter controls. These programs should promote a strong risk management culture, enhance risk awareness, and ensure adherence to the established policies and procedures.
- 6. **Policy Review** This policy shall be reviewed periodically, at least annually, or as deemed necessary, to ensure its relevance and effectiveness. Any updates or amendments to this policy shall be approved by senior management and communicated to all relevant parties.
- 7. **Non-Compliance** Failure to comply with this policy may result in disciplinary action, including but not limited to, warnings, suspension, termination, or legal action, as deemed appropriate based on the severity of non-compliance.

By adhering to this Risk Parameter Controls Policy, **VT Capital Market Pvt Ltd** aims to proactively identify and manage risks.

Policy Title: Technical Glitch Handling PolicyEffective Date: [25th Aug 2025]

1. **Purpose** The purpose of this policy is to establish guidelines and procedures for handling technical glitches that may arise within the information technology infrastructure and systems of VT Capital Market Pvt Ltd. This policy aims to minimize disruptions, ensure timely resolution of technical issues, and maintain the integrity and security of the Company's operations.
2. **Scope** This policy applies to all employees, contractors, and third-party service providers who are responsible for the management, maintenance, and support of the Company's information technology systems.
3. **Definitions**
 - a. **Technical Glitch:** An unexpected malfunction or disruption in the Company's information technology systems that affects its normal functioning, performance, or availability.
 - b. **Incident:** An event or occurrence resulting in a disruption or potential disruption to the Company's information technology systems and services.
4. **Incident Reporting and Escalation**
 - a. **Reporting**
 - i) All technical glitches and incidents must be promptly reported to the designated IT support team through the approved channels (e.g., help desk, incident reporting system).
 - ii) Employees should provide detailed information about the symptoms, impact, and any relevant error messages associated with the technical glitch.
 - b. **Categorization and Prioritization**
 - i) The IT support team shall categorize incidents based on their impact, urgency, and severity.
 - ii) A prioritization framework should be established to determine the order of incident resolution based on business needs and criticality.
 - c. **Escalation**
 - i) Incidents should be escalated to higher-level support teams or management based on predefined escalation procedures.
 - ii) Escalation criteria may include the severity of the incident, its potential impact on business operations, or failure to meet defined service level agreements (SLAs).
 - iii) Escalation paths and contact details should be clearly communicated and readily accessible to all relevant personnel.
5. **Incident Management and Resolution**
 - a. **Incident Handling**
 - i) The IT support team shall promptly acknowledge and initiate the incident handling process upon receipt of the incident report.
 - ii) Incidents should be assigned to appropriate personnel with the necessary expertise to investigate, diagnose, and resolve the technical glitch.

b. Documentation and Tracking

- i) All incidents should be accurately documented, including relevant details such as incident description, investigation findings, actions taken, and resolution outcomes.
- ii) Incident tracking systems or tools should be used to monitor the status and progress of incident resolution, ensuring timely updates and effective coordination.

c. Resolution and Recovery

- i) The IT support team shall work diligently to resolve technical glitches and restore normal system functionality within defined service level targets.
- ii) Adequate resources, including technical expertise and necessary equipment, should be allocated to expedite incident resolution.
- iii) Where applicable, backup systems or contingency plans should be activated to minimize disruptions and ensure business continuity.

6. Communication and Notification**a. Stakeholder Communication**

- i) Regular and transparent communication should be maintained with relevant stakeholders (e.g., Employees, clients, regulatory bodies) regarding the incident, its impact, and the progress of Resolution efforts.
- ii) Communication channels may include email updates, notifications through the Company's website or client portals, or dedicated incident communication platforms.

b. Notification of Critical Incidents

- i) Critical incidents, particularly those impacting critical business operations or sensitive customer data, should be promptly reported to senior management and the appropriate regulatory authorities as required by applicable laws and regulations.

7. Incident Analysis and Improvement**a. Post-Incident Analysis**

- i) A post-incident analysis should be conducted to identify the root causes, contributing factors, and lessons learned from each technical glitch.
- ii) The findings of the analysis should be used to implement preventive measures and enhance.

8. Technical Glitch Prevention and Continuous Improvement**a. Root Cause Analysis**

- i) After resolving incidents, the Company should conduct root cause analysis to identify underlying causes and contributing factors.
- ii) Remedial actions and preventive measures should be implemented to address root causes and minimize the recurrence of similar technical glitches.

b. Performance Monitoring and Maintenance

- i) Regular monitoring of systems, networks, and infrastructure should be conducted to proactively identify and address potential technical issues or vulnerabilities.
- ii) Scheduled maintenance activities, including patching, upgrades, and hardware checks, should be performed to ensure system stability and reliability.

c. Training and Knowledge Sharing

- i) Ongoing training and knowledge sharing sessions should be conducted to enhance the technical skills and troubleshooting capabilities of employees involved in incident resolution.
- ii) Best practices and lessons learned from incident handling should be shared with relevant teams or departments to improve overall incident response effectiveness.

9. **Policy Review and Compliance**

a. Policy Review

- i) This technical glitch handling policy shall be reviewed periodically, at least annually, or as deemed necessary, to ensure its relevance, effectiveness, and alignment with industry best practices.
- ii) Any updates or amendments to this policy shall be approved by senior management and communicated to all relevant parties.

b. Non-Compliance

- i) Failure to comply with this policy may result in disciplinary action, including but not limited to warnings, suspension, termination, or legal action, as deemed appropriate based on the severity of non-compliance.

By adhering to this Technical Glitch Handling Policy, **VT Capital Market Private Limited** aims to ensure prompt and efficient resolution of technical glitches, minimize disruption to business operations, and maintain the integrity and availability of systems and services.

Policy Title: Application Software Policy

Effective Date: [25th Aug 2025]

1. Purpose The purpose of this policy is to establish guidelines and procedures for the management, procurement, and use of application software within **VT Capital Market Private Limited**. This policy aims to ensure the efficient and secure utilization of application software while maintaining compliance with relevant laws, regulations, and industry best practices.
2. Scope This policy applies to all employees, contractors, and third-party service providers who are involved in the acquisition, deployment, maintenance, and use of application software within the Company.
3. Definitions
 - a. Application Software: Computer programs, including both commercial off-the-shelf (COTS) and custom-developed software, designed to perform specific tasks or functions to support business operations.
 - b. Software Acquisition: The process of obtaining application software licenses or subscriptions, either through purchase, lease, or open-source distribution.
 - c. Software Deployment: The process of installing, configuring, and integrating application software into the Company's information technology infrastructure.

- d. Software Maintenance:
Ongoing activities that include software updates, patches, bug fixes, performance optimization, and vendor support.

4. Software Governance

a. Software Inventory

- i. The Company shall maintain an up-to-date inventory of all application software used within the organization.
- ii. The inventory should include details such as software name, version, license details, vendor information, and deployment status.

b. Software Approval Process

- i) All software acquisitions, whether through purchase, lease, or open-source distribution, must undergo an approval process.
- ii) The approval process should include a review of the software's functionality, compatibility, security, licensing terms, and compliance with the Company's policies and standards.
- iii) Approval for software acquisitions should be obtained from the appropriate department or management level, considering the budgetary and operational impacts.

c. Licensing Compliance

- i) The Company shall ensure compliance with software licensing agreements and intellectual property rights.
- ii) Unauthorized installation, duplication, distribution, or use of software is strictly prohibited.
- iii) Regular audits should be conducted to verify software licenses and ensure compliance with contractual obligations.

d. Software Version Control

- i) The Company shall establish processes for managing software versions and upgrades.
- ii) Outdated software versions should be identified and upgraded to maintain compatibility, security, and supportability.
- iii) Standardized version control practices should be implemented to avoid compatibility issues and security vulnerabilities.

Software Deployment and Configuration

Security Considerations

- i) Application software deployments should adhere to the Company's information security policies and standards.
- ii) Secure configurations, including appropriate access controls, authentication mechanisms, encryption, and data protection, should be implemented during software deployment.

Testing and Quality Assurance

- i) Application software should undergo thorough testing and quality assurance procedures before deployment.
- ii) Testing should encompass functional testing, performance testing, security testing, and compatibility testing, as appropriate.

c. Change Management

- i) Software deployments and updates should follow the Company's change management process.
- ii) Change requests for software deployment or configuration changes should be appropriately documented, reviewed, approved, and tracked.

6. Software Maintenance and Support

a. Patch Management

- i) The Company shall establish a patch management process to address vulnerabilities and apply software updates in a timely manner.
- ii) Critical security patches should be prioritized and applied promptly to mitigate security risks.

b. Vendor Support

- i) The Company should maintain a valid support agreement with software vendors to ensure timely access to technical support, bug fixes, and software updates.
- ii) Vendor support contacts and procedures should be readily accessible to relevant personnel.

c. Monitoring and Performance Optimization

- i) Ongoing monitoring of software performance and utilization.

d. Software Compliance and Auditing

- i) The Company shall conduct periodic audits to ensure compliance with software licensing agreements and usage policies.
- ii) Any unauthorized or unlicensed software installations should be identified and addressed promptly.

7. User Education and Awareness

a. Software Usage Guidelines

- i) The Company shall provide employees with guidelines on the acceptable use of application software, including restrictions on installing unauthorized software or engaging in software piracy.

b. Security Awareness Training

- i) Employees should receive regular security awareness training, including best practices for secure software usage, recognizing phishing attempts, and reporting suspicious activities.

8. Policy Review and Compliance

a. Policy Review

- i) This Application Software Policy shall be reviewed periodically, at least annually, or as deemed necessary, to ensure its relevance, effectiveness, and alignment with industry best practices.
- ii) Any updates or amendments to this policy shall be approved by senior management and communicated to all relevant parties.

VT CAPITAL MARKET PVT. LTD.
Sain
Director

- b. Non-Compliance . Failure to comply with this policy may result in disciplinary action, including but not limited to warnings, suspension, termination, or legal action, as deemed appropriate based on the severity of non-compliance.

By adhering to this Application Software Policy, **VT Capital Market Private Limited** aims to ensure the efficient and secure management of application software, promote compatibility and interoperability, and maintain compliance with legal and licensing requirements.

Policy Title: Information Security Policy

Effective Date: [25th Aug 2025]

1. Purpose The purpose of this policy is to establish guidelines and procedures for the protection and security of information assets within **VT Capital Market Private Limited** . This policy aims to ensure the confidentiality, integrity, and availability of information, safeguard against unauthorized access or disclosure, and comply with relevant laws, regulations, and industry best practices.
2. Scope This policy applies to all employees, contractors, third-party service providers, and any individuals who have access to the Company's information assets.
3. Definitions

a. Information Assets:

Any data, information, systems, networks, or resources that are owned, controlled, or used by the Company in the course of its operations.

b. Confidentiality:

The protection of information from unauthorized disclosure to ensure its secrecy and prevent unauthorized access.

c. Integrity:

The accuracy, completeness, and reliability of information, as well as the safeguarding against unauthorized modification or alteration.

d. Availability:

The accessibility and usability of information and information systems to authorized individuals when needed.

4. Information Security Governance

a) Roles and Responsibilities

- i. The Company shall designate responsible individuals for information security governance, including the appointment of an Information Security Officer (ISO).
- ii. Roles, responsibilities, and reporting lines for information security management shall be clearly defined and communicated to all employees.

b) Risk Management

- i. The Company shall conduct regular risk assessments to identify and evaluate information security risk.
- ii. Risk mitigation strategies and controls shall be implemented to address identified risks, considering their impact and likelihood.

c) Compliance

- i. The Company shall comply with all applicable laws, regulations, contractual obligations, and industry standards related to information security.
- ii. Regular reviews and audits should be conducted to ensure compliance with information security requirements.

5. Information Classification and Handling

a) Information Classification

- i. The Company shall classify information assets based on their sensitivity, value, and criticality.
- ii. Classification levels should be defined, such as confidential, internal use only, and public, to guide appropriate handling and protection measures.

b) Access Control

- i. Access to information assets shall be granted on a need-to-know basis, considering job roles, responsibilities, and business requirements.
- ii. User access privileges should be reviewed regularly, and access should be promptly revoked upon termination or change in job responsibilities.

c) Data Protection

- i. The Company shall implement appropriate measures to protect information assets from unauthorized access, loss, destruction, alteration, or disclosure.
- ii. Encryption, secure storage, backup and recovery procedures, and strong authentication mechanisms should be employed to safeguard sensitive information.

d) Information Sharing

- i. Information sharing, both internally and externally, should be conducted in accordance with the Company's policies and procedures.
- ii. Agreements, contracts, or non-disclosure agreements (NDAs) may be required when sharing information with third parties.

6. Information Technology Security

a) Network and Infrastructure Security

- i. The Company shall implement secure network architecture, firewalls, intrusion detection/prevention systems, and other security measures to protect the integrity and availability of information assets.

b) System Access Control

- i. Access to information systems and applications should be controlled through user authentication mechanisms, such as strong passwords, multi-factor authentication, and least privilege principles.

c) Malware Protection

- i. The Company shall deploy and maintain up-to-date anti-malware solutions to detect and prevent malware infections.

d) Incident Response

- i. The Company shall establish an incident response process to detect, respond to, and recover from information security incidents.

- ii. Employees should be educated on reporting procedures and their responsibilities in reporting and escalating security incidents.

7. Security Awareness and Training

a) Security Awareness Program

- i. The Company shall implement a security awareness program to educate employees about information security risks, best practices, and their responsibilities in safeguarding information assets.
- ii. Regular training sessions, awareness campaigns, and communication materials should be provided to promote a security-conscious culture.

b) Incident Reporting and Response Training

- i. Employees shall be trained on the proper procedures for reporting information security incidents promptly and accurately.
- ii. Training programs should cover incident response roles, responsibilities, and the escalation process.

8. Policy Review and Compliance

a) Policy Review

- i. This policy shall be reviewed periodically, at least annually, or as deemed necessary, to ensure its relevance and effectiveness.
- ii. Any updates or amendments to this policy shall be approved by senior management and communicate to all relevant parties

b) Non-Compliance

- i. Failure to comply with this policy may result in disciplinary action, including but not limited to warnings, suspension, termination, or legal action, as deemed appropriate based on the severity of non-compliance.

By adhering to this Information Security Policy, **VT Capital Market Private Limited** aims to protect its information assets and maintain the trust and confidence of its clients and stakeholders.

Policy Title: Password PolicyEffective Date: [25th Aug 2025]

1. **Purpose** The purpose of this policy is to establish guidelines and best practices for the creation, management, and protection of passwords within **VT Capital Market Pvt Ltd**. This policy aims to ensure the confidentiality, integrity, and security of information assets by promoting strong and secure passwords, minimizing the risk of unauthorized access or disclosure.
2. **Scope** This policy applies to all employees, contractors, third-party service providers, and any individuals who have access to the Company's systems, applications, and information assets.
3. **Password Creation and Complexity**
 - a. Password Strength
 - i) Passwords must meet minimum complexity requirements to prevent easy guessing or cracking.
 - ii) Passwords should be a minimum of eight characters in length and include a combination of uppercase letters, lowercase letters, numbers, and special characters.
 - b. Password Uniqueness
 - i. Each user must have a unique password for their individual accounts.
 - ii. Reusing passwords across multiple systems or accounts is strictly prohibited.
 - c. Password Expiration
 - i) Passwords should be changed regularly to enhance security.
 - ii) The Company shall define a maximum password age, after which users will be required to change their passwords.
4. **Password Management**
 - a. Password Storage
 - i. Passwords must never be stored in clear text or easily accessible locations.
 - ii. Passwords should be stored using strong encryption techniques.
 - b. Password Sharing
 - i) Sharing passwords with others, including colleagues or non-authorized individuals, is strictly prohibited.
 - ii) Each user is responsible for maintaining the confidentiality of their password.
 - c. Password Reset
 - i) Password reset processes should be in place to allow users to reset their passwords securely in the event of forgotten or compromised passwords.
 - ii) Users must follow the prescribed password reset procedures and authenticate their identity before changing passwords.

5. Multi-Factor Authentication (MFA)

a. MFA Implementation

- i) Multi-Factor Authentication should be implemented for critical systems, privileged accounts, or accounts with access to sensitive information.
- ii) MFA adds an additional layer of security by requiring users to provide multiple authentication factors such as a password and a unique code sent to their registered device.

6. User Education and Awareness

a. Password Best Practices

- i) The Company shall provide training and awareness programs to educate users on password best practices.
- ii) Training materials and resources should cover topics such as password creation, password protection and recognizing phishing or social engineering attempts.

b. Phishing Awareness

- i) Users should be educated about the risks associated with phishing attacks and how to identify and report suspicious emails, links, or requests for passwords.

7. Password Policy Enforcement

a. Monitoring and Compliance

- i) The Company reserves the right to monitor password usage, detect weak passwords, and enforce password policy compliance.
- ii) Non-compliance with this policy may result in disciplinary actions, including but not limited to warnings, suspension, termination, or legal action, as deemed appropriate.

b. Policy Review

- i) This password policy shall be reviewed periodically, at least annually, or as deemed necessary, to ensure its relevance, effectiveness, and alignment with industry best practices.

By following this Password Policy, VT Capital Market Pvt Ltd aims to enhance the security of its systems, protect confidential information, and mitigate the risk of unauthorized access or data breaches.

Policy Title: Network Security PolicyEffective Date: [25th Aug 2025]

1. **Purpose** The purpose of this policy is to establish guidelines and procedures for the secure configuration, management, and protection of the network infrastructure within **VT Capital Market Pvt Ltd**. This policy aims to ensure the confidentiality, integrity, and availability of network resources, prevent unauthorized access or data breaches, and comply with relevant laws, regulations, and industry best practices.
2. **Scope** This policy applies to all employees, contractors, third-party service providers, and any individuals who have access to the Company's network infrastructure or utilize network resources.
3. **Network Infrastructure Security**
 - a. Network Architecture
 - i) The Company shall maintain a secure network architecture that segregates network segments based on security requirements.
 - ii) Network segmentation should be implemented to restrict access and limit the impact of potential security incidents.
 - b. Perimeter Security
 - i) Firewalls, intrusion detection/prevention systems, and other appropriate security controls shall be deployed at the network perimeter to protect against unauthorized access and malicious activities.
 - ii) Network traffic entering or leaving the Company's network should be monitored and filtered to prevent unauthorized or malicious communication.
 - c. Wireless Network Security
 - i) Wireless networks shall be implemented with strong encryption (e.g., WPA2 or WPA3) and secure authentication mechanisms (e.g., EAP-TLS) to protect against unauthorized access and data interception.
 - ii) Wireless access points should be regularly patched, monitored, and managed to prevent vulnerabilities.
 - d. Remote Network Access
 - i) Remote access to the Company's network should be protected using secure methods, such as virtual private networks (VPNs) with strong encryption and multi-factor authentication.
 - ii) Remote access permissions should be granted on a need-to-know basis and reviewed regularly.
4. **Network Monitoring and Logging**
 - a. Network Traffic Monitoring
 - i) The Company shall implement network monitoring tools to detect and analyze network traffic for signs of unauthorized access, anomalies, or malicious activities.
 - ii) Intrusion detection/prevention systems, log analyzers, and other monitoring mechanisms should be deployed to proactively identify potential security incidents.

b. Log Management

- i) Logs generated by network devices, servers, and security systems should be collected, stored, and analyzed for security and compliance purposes.
- ii) Log management systems should be implemented to ensure the availability, integrity, and confidentiality of log data.

c. Incident Response

- i) The Company shall establish an incident response process to promptly detect, respond to, and mitigate network security incidents.
- ii) Employees should be educated on reporting procedures and their responsibilities in reporting and escalating network security incidents.

5. Access Control and Authentication**a. User Access Control**

- i) Access to network resources, systems, and sensitive information should be granted on a need-to-know and least privilege basis.
- ii) User access privileges should be reviewed regularly, and access should be promptly revoked upon termination or change in job responsibilities.

b. Network Device Authentication

- i) Network devices, such as switches, routers, and wireless access points, should be configured with strong authentication mechanisms, including unique, complex passwords or digital certificates.
- ii) Default passwords should be changed immediately upon device deployment.

6. Network Vulnerability Management**a. Patch Management**

- i) The Company shall implement a patch management process to ensure timely installation of security patches for network devices, operating systems, and applications.
- ii) Critical security patches should be prioritized and applied promptly to mitigate known vulnerabilities.

b. Network Device Configuration

- i) Network devices should be configured securely, following industry best practices and vendor recommendations.
- ii) Default configurations, unnecessary services, or insecure protocols should be disabled or removed.

7. Policy Review and Compliance**a. Policy Review**

- i) This network security policy shall be reviewed periodically, at least annually, or as deemed necessary, ensure its relevance, effectiveness, and alignment with changing threats and technologies.
- ii) Any updates or amendments to this policy shall be approved by senior management and communicated to all relevant parties.

b. Compliance

- i) The Company shall regularly assess its network infrastructure against industry standards, best practices, and regulatory requirements to ensure compliance.
- ii) Network security audits, vulnerability assessments, and penetration testing should be conducted to identify and address any security gaps or weaknesses.

By adhering to this Network Security Policy, **VT Capital Market Pvt Ltd** aims to protect its network infrastructure, prevent unauthorized access or data breaches, and maintain the confidentiality, integrity and availability of network resources.

Policy Title: Cyber Security Policy

Effective Date: [25th Aug 2025]

1. Purpose The purpose of this policy is to establish guidelines and procedures to protect the information assets and digital infrastructure of **VT Capital Market Private Limited** from unauthorized access, use, disclosure, disruption, modification, or destruction. This policy aims to ensure the confidentiality, integrity, and availability of the Company's information assets and mitigate the risks associated with cyber threats:
2. Scope This policy applies to all employees, contractors, and third-party service providers who have access to the Company's information assets or utilize the Company's digital infrastructure.
3. Information Security Governance
 - a. Roles and Responsibilities
 - i) The Company shall define and communicate the roles and responsibilities of employees and stakeholders regarding cyber security.
 - ii) Designated individuals or teams shall be responsible for overseeing and implementing the cyber security measures outlined in this policy.
 - b. Risk Assessment and Management
 - i) The Company shall conduct periodic risk assessments to identify and evaluate cyber security risks.
 - ii) Mitigation measures, safeguards, and controls shall be implemented to manage and reduce identified risks.
 - c. Incident Response and Recovery
 - i) The Company shall establish an incident response plan that outlines the procedures for detecting, reporting, and responding to cyber security incidents.
 - ii) The plan should include steps for containment, investigation, mitigation, recovery, and communication of incidents.
4. Access and Authentication Controls
 - a. User Access Management
 - i) User access to systems, networks, and data shall be granted based on the principle of least privilege.
 - ii) User access requests shall be reviewed and approved by authorized personnel.
 - b. Password Management
 - i) Strong password policies shall be enforced, including the use of complex passwords, regular password changes, and password encryption.
 - ii) Multi-factor authentication shall be implemented for critical systems and privileged accounts.

c. User Account Termination

- i) User accounts shall be promptly deactivated or removed upon termination or change in job responsibilities.
- ii) Regular audits shall be conducted to ensure that inactive accounts are disabled or removed.

5. Network and Infrastructure Security

a. Network Perimeter Protection

- i) Firewalls, intrusion prevention systems, and other appropriate security measures shall be implemented to protect the Company's network perimeter.
- ii) Regular updates and monitoring of perimeter security controls shall be performed.

b. Data Encryption

- i) Sensitive data in transit, such as customer information or financial data, shall be encrypted using secure protocols.
- ii) Encrypted storage solutions shall be utilized for sensitive data at rest, including backups and archives.

c. Network Monitoring and Intrusion Detection

- i) The Company shall implement network monitoring tools and intrusion detection systems to detect and respond to suspicious network activities.
- ii) Logs and alerts from network monitoring systems shall be regularly reviewed and analyzed.

6. Information Security Awareness and Training

a. Employee Training and Education

- i) All employees shall receive regular training and awareness programs on cyber security best practices, policies, and procedures.
- ii) Training sessions shall cover topics such as phishing awareness, social engineering, password security, and safe browsing habits.

b. Reporting Security Incidents

- i) Employees shall be encouraged to report any suspected or actual cyber security incidents promptly.
- ii) Reporting channels and procedures shall be communicated and readily accessible to all employees.

7. Vendor and Third-Party Management

a. Due Diligence

- i) The Company shall conduct due diligence and risk assessments of vendors and third-party service providers who have access to the Company's information assets.
- ii) Contracts and agreements shall include provisions for data protection, confidentiality, and security requirements.

b. Monitoring and Oversight

- i) Ongoing monitoring of vendors and third parties shall be conducted to ensure compliance with cyber security requirements and industry standards.
- ii) Periodic security assessments and audits of vendor systems and processes may be performed.

8. Policy Review and Compliance

a. Policy Review

- i) This Cyber Security Policy shall be reviewed periodically, at least annually, or as deemed necessary, to ensure its relevance, effectiveness, and alignment with industry best practices.
- ii) Any updates or amendments to this policy shall be approved by senior management and communicated to all relevant parties.

b. Non-Compliance

- i) Failure to comply with this policy may result in disciplinary action, including but not limited to warnings, suspension, termination, or legal action, as deemed appropriate based on the severity of non-compliance.

By adhering to this Cyber Security Policy, **VT Capital Market Private Limited** aims to protect its information assets, safeguard against cyber threats, and maintain the confidentiality, integrity, and availability of its digital infrastructure.

Policy Title: Backup Policy

Effective Date: [25th Aug 2025]

1. Purpose The purpose of this policy is to establish guidelines and procedures for the backup and recovery of critical data and systems within **VT Capital Market Private Limited**. This policy aims to ensure the availability, integrity, and recoverability of data assets, mitigate the risk of data loss, and facilitate efficient data restoration in the event of data loss or system failure.
2. Scope This policy applies to all employees, contractors, and third-party service providers who are responsible for managing or utilizing the Company's data assets and systems.

3. Backup Strategy

a. Data Classification

- i) The Company shall classify data based on its criticality, sensitivity, and business impact.
- ii) Data classification shall determine the frequency and level of backup and the retention period for each data category.

b. Backup Frequency

- i) Regular backups shall be performed based on the data classification and business requirements.
- ii) Critical data and systems shall be backed up more frequently, while less critical data may have less frequent backup intervals.

c. Data Retention

- i) Backup retention periods shall be defined based on legal, regulatory, and business requirements.
- ii) Retention periods should be aligned with data classification and comply with applicable data protection and privacy regulations.

d. Backup Storage and Locations

- i) Backup data shall be stored in secure and reliable storage systems, both on-premises and off-site.
- ii) Off-site backups should be located in a geographically separate location to ensure data redundancy and protection against physical disasters.

e. Backup Integrity and Validation

- i) Backup processes and procedures shall include integrity checks and validation to ensure the completeness and accuracy of backup data.
- ii) Regular tests and audits of backup systems and processes should be conducted to verify the recoverability of data.

4. Backup Procedures

a. Backup Schedule

- i) A backup schedule shall be established, specifying the timing, frequency, and duration of backup operations.
- ii) Backup schedules should be reviewed and updated periodically to accommodate changes in data volumes and business requirements.

b. Backup Methods and Technologies

- i) The Company shall utilize reliable and proven backup methods and technologies suitable for the backup and recovery of data and systems.
- ii) Backup solutions may include disk-based backups, tape backups, cloud backups, or a combination thereof.

c. Backup Monitoring and Reporting

- i) Backup operations shall be monitored to ensure their successful completion.
- ii) Backup logs and reports should be generated and reviewed regularly to identify any failures, errors, or anomalies in the backup process.

d. Off-site Backup Rotation

- i) Off-site backup media or data should be rotated and stored securely in accordance with the backup retention policies.
- ii) Rotation schedules and procedures should be documented and followed to ensure the availability and recoverability of off-site backups.

5. Backup Recovery

a. Recovery Point Objectives (RPO) and Recovery Time Objectives (RTO)

- i) The Company shall establish RPO and RTO targets based on the criticality of data and systems.
- ii) RPO defines the acceptable data loss window, while RTO specifies the maximum tolerable downtime for systems and services.

b. Recovery Testing

- i) Regular backup recovery testing shall be conducted to validate the recoverability and effectiveness of backup procedures.
- ii) Testing should include both partial and full data/system recovery scenarios.

c. Disaster Recovery Plan

- i) The Company shall maintain a comprehensive disaster recovery plan that outlines the procedures and processes for restoring critical systems and data in the event of a disaster or major incident.
- ii) The plan should include contact information, roles and responsibilities, recovery priorities, and communication protocols.

6. Policy Review and Compliance

a. Policy Review

- i) This Backup Policy shall be reviewed periodically, at least annually, or as deemed necessary, to ensure its relevance, effectiveness, and alignment with industry best practices.
- ii) Any updates or amendments to this policy shall be approved by senior management and communicated to all relevant parties.

b. Non-Compliance

- i) Failure to comply with this policy may result in disciplinary action, including but not limited to warnings, suspension, termination, or legal action, as deemed appropriate based on the severity of non-compliance.

By adhering to this Backup Policy, **VT Capital Market Private Limited** aims to ensure the availability and recoverability of critical data and systems, minimize the risk of data loss, and maintain business continuity in the face of data-related incidents or system failures.

Policy Title: Remote Access Control Policy

Effective Date: [25th Aug 2025]

1. Purpose The purpose of this policy is to establish guidelines and procedures for secure remote access to **VT Capital Market Private Limited** resources. This policy aims to ensure the confidentiality, integrity, and availability of Company information assets while allowing authorized individuals to access and use these resources remotely.
2. Scope This policy applies to all employees, contractors, and third-party service providers who require remote access to the Company's resources, including networks, systems, applications, and data.
3. Remote Access Controls

a. User Authentication

- i) Remote access to Company resources shall require strong user authentication mechanisms, such as unique usernames and complex passwords.
- ii) Multi-factor authentication (MFA) should be implemented for enhanced security.

b. Access Authorization

- i) Access to specific resources and systems shall be granted based on job roles, responsibilities, and the principle of least privilege.
- ii) Access requests must be approved by authorized personnel before granting remote access.

c. Secure Remote Connection

- i) Remote access connections shall be established using secure protocols, such as Secure Shell (SSH), Secure Sockets Layer/Transport Layer Security (SSL/TLS), or Virtual Private Network (VPN) technologies.
- ii) Unsecured or outdated protocols, such as Telnet or unencrypted remote desktop protocols, shall not be used.

d. Endpoint Security

- i) All remote devices used for accessing Company resources shall comply with the Company's endpoint security policies and standards.
- ii) Endpoint security measures should include up-to-date antivirus software, firewalls, and regular system patching.

e. Data Encryption

- i) Data transmitted between remote devices and Company resources shall be encrypted using strong encryption algorithms.
- ii) Encryption should be applied to both data in transit and data stored on remote devices.

f. Session Timeout and Idle Disconnect

- i) Remote access sessions shall have idle timeout and automatic disconnect mechanisms in place to minimize the risk of unauthorized access in case of inactivity.

4. Remote Access Monitoring**a. Logging and Auditing**

- i) Remote access activities shall be logged and audited to monitor for unauthorized access attempts, suspicious activities, and compliance with the Remote Access Control Policy.
- ii) Log data should be regularly reviewed and retained in accordance with applicable legal and regulatory requirements.

b. Intrusion Detection and Prevention

- i) Intrusion detection and prevention systems shall be implemented to monitor and block malicious or unauthorized remote access attempts.
- ii) Alerts from intrusion detection systems should be promptly reviewed and responded to.

5. User Awareness and Training**a. Remote Access Guidelines**

- i) Employees shall be provided with clear guidelines and procedures for remote access, including acceptable use policies, security best practices, and responsibilities while accessing Company resources remotely.
- ii) Employees shall be made aware of the risks associated with remote access and educated on how to mitigate those risks.

b. Security Awareness Training

- i) Regular security awareness training programs shall be conducted to educate employees about remote access security, password hygiene, phishing awareness, and other relevant topics.

6. Policy Review and Compliance

a. Policy Review

- i) This Remote Access Control Policy shall be reviewed periodically, at least annually, or as deemed necessary, to ensure its relevance, effectiveness, and alignment with industry best practices.
- ii) Any updates or amendments to this policy shall be approved by senior management and communicated to all relevant parties.

b. Non-Compliance

- i) Failure to comply with this policy may result in disciplinary action, including but not limited to warnings, suspension, termination, or legal action, as deemed appropriate based on the severity of non-compliance.

By adhering to this Remote Access Control Policy, **VT Capital Market Private Limited** aims to ensure secure remote access to its resources, protect sensitive information, and maintain the confidentiality, integrity, and availability of Company data and systems.

Policy Title: Audit Trail Policy

Effective Date: [25th Aug 2025]

1. Purpose The purpose of this policy is to establish guidelines and procedures for the creation, retention, and review of audit trails within **VT Capital Market Private Limited**. This policy aims to ensure the integrity, confidentiality, and availability of audit trail data, as well as facilitate effective monitoring, investigation, and compliance with regulatory requirements.

2. Scope This policy applies to all employees, contractors, and third-party service providers who have access to or are responsible for generating, managing, or reviewing audit trail data within the Company.

3. Audit Trail Requirements

a. Definition and Scope

- i) Audit trails are records of activities and events that capture relevant information regarding user actions, system events, and data changes.
- ii) Audit trails shall cover all critical systems, applications, and data repositories that contain sensitive or regulated information.

b. Logging and Capture

- i) Relevant events and activities shall be logged and captured in the audit trail.
- ii) The audit trail should include information such as date and time stamps, user IDs, IP addresses, system activities, and data changes.

c. Integrity and Protection

- i) Audit trails shall be protected against unauthorized access, modification, deletion, or tampering.
- ii) Access controls, encryption, and secure storage measures shall be implemented to ensure the integrity and confidentiality of audit trail data.

d. Retention Period

- i) The retention period for audit trail data shall comply with legal, regulatory, and business requirements.
- ii) Retention periods should be defined based on the sensitivity of the data, industry standards, and any specific regulatory obligations.

e. Backup and Recovery

- i) Adequate backup and recovery mechanisms shall be implemented to protect audit trail data from loss or corruption.
- ii) Regular testing of backup and recovery procedures should be conducted to ensure the availability and integrity of audit trail data.

4. Audit Trail Monitoring and Review

a. Monitoring and Alerting

- i) Real-time monitoring of audit trail data should be implemented to identify suspicious or unauthorized activities promptly.
- ii) Alert mechanisms should be in place to notify appropriate personnel in the event of potential security incidents or policy violations.

b. Log Analysis and Review

- i) Regular analysis and review of audit trail data should be conducted to detect anomalies, security breaches, or compliance violations.
- ii) Logs should be analyzed using appropriate log management and analysis tools to identify patterns or indicators of compromise.

c. Incident Investigation

- i) Audit trail data shall be used as a critical resource for investigating security incidents, unauthorized access, or data breaches.
- ii) Incident response teams should have access to and expertise in analyzing audit trail data to facilitate effective incident response and recovery.

5. Policy Review and Compliance

a. Policy Review

- i) This Audit Trail Policy shall be reviewed periodically, at least annually, or as deemed necessary, to ensure its relevance, effectiveness, and alignment with industry best practices.
- ii) Any updates or amendments to this policy shall be approved by senior management and communicated to all relevant parties.

b. Non-Compliance

- i) Failure to comply with this policy may result in disciplinary action, including but not limited to warnings, suspension, termination, or legal action, as deemed appropriate based on the severity of non-compliance.

By adhering to this Audit Trail Policy, **VT Capital Market Private Limited** aims to maintain the integrity of its systems and data, detect and respond to security incidents, meet regulatory requirements, and support accountability and transparency in its operations.

Policy Title: Change Management Policy

Effective Date: [25th Aug 2025]

1. **Purpose** The purpose of this policy is to establish guidelines and procedures for managing change to systems, applications, infrastructure, and processes within **VT Capital Market Private Limited**. This policy aims to minimize the risk of disruptions, errors, and security incidents caused by unauthorized or poorly managed changes, and to ensure that changes are implemented in a controlled and standardized manner.
2. **Scope** This policy applies to all employees, contractors, and third-party service providers who are involved in initiating, planning, approving, implementing, or reviewing changes within the Company's IT environment.

3. Change Management Process

a. Change Request

- i) All changes, whether planned or unplanned, shall be documented and submitted as change requests using the designated change management system.
- ii) Change requests should include a clear description of the change, its purpose, scope, and expected outcomes.

b. Change Categorization and Prioritization

- i) Changes shall be categorized based on their impact, urgency, and risk level.
- ii) Prioritization of changes should consider factors such as business impact, security implications, and regulatory compliance requirements.

c. Change Approval and Authorization

- i) Changes shall undergo a formal approval process based on their category and impact.
- ii) Authorized individuals or change advisory boards should review and approve changes to ensure alignment with business objectives and compliance with policies and procedures.

d. Change Planning and Documentation

- i) Changes shall be thoroughly planned, including detailed implementation steps, rollback plans, and testing requirements.
- ii) Change documentation should include change descriptions, implementation plans, risk assessments, and any necessary approvals or sign-offs.

e. Change Testing

- i) Changes that could impact system stability, security, or performance shall undergo testing in a controlled environment.
- ii) Testing procedures and results should be documented and reviewed before proceeding with the change implementation.

f. Change Implementation

- i) Changes shall be implemented during approved maintenance windows or designated change windows to minimize disruptions.
- ii) Proper coordination, communication, and change control procedures should be followed during the implementation process.

g. Change Review and Evaluation

- i) Changes should be reviewed and evaluated after implementation to assess their effectiveness and impact on systems, processes, and users.
- ii) Lessons learned from changes should be documented and incorporated into future change management practices.

4. **Change Communication and Training**

a. Stakeholder Communication

- i) Appropriate stakeholders, including users, management, and affected teams, should be informed of upcoming changes, their impact, and any necessary actions or precautions.
- ii) Clear and timely communication should be maintained throughout the change management process.

b. Training and Awareness

- i) Employees involved in the change management process should receive training on change management principles, procedures, and tools.
- ii) Ongoing awareness programs should be conducted to ensure that employees understand the importance of change management and their roles in the process.

5. **Policy Review and Compliance**

a. Policy Review

- i) This Change Management Policy shall be reviewed periodically, at least annually, or as deemed necessary, to ensure its relevance, effectiveness, and alignment with industry best practices.
- ii) Any updates or amendments to this policy shall be approved by senior management and communicated to all relevant parties.

b. Non-Compliance

- i) Failure to comply with this policy may result in disciplinary action, including but not limited to warnings, suspension, termination, or legal action, as deemed appropriate based on the severity of non-compliance.

By adhering to this Change Management Policy, **VT Capital Market Private Limited** aims to ensure the smooth and controlled implementation of changes, minimize disruptions, enhance system reliability and security, and support the continuous improvement of its IT environment.

Policy Title: User Management and Access Control Policy

Effective Date: [25th Aug 2025]

1. Purpose The purpose of this policy is to establish guidelines and procedures for user management and access control within VT Capital Market Private Limited ("the Company"). This policy aims to ensure the confidentiality, integrity, and availability of Company resources by granting appropriate access rights to authorized individuals while preventing unauthorized access, data breaches, and insider threats.
2. Scope This policy applies to all employees, contractors, third-party service providers, and any other individuals who require access to Company systems, applications, networks, and data.
3. **User Account Management**
 - a. User Account Provisioning
 - i) User accounts shall be created only for authorized individuals based on their job roles, responsibilities, and the principle of least privilege.
 - ii) User account provisioning should follow a formal process, including verification of user identity, approval from appropriate authorities, and assignment of access privileges.
 - b. Access Rights and Permissions
 - i) Access rights and permissions shall be granted to users based on their job functions and specific requirements.
 - ii) Access privileges should be regularly reviewed and updated to align with changes in job roles or responsibilities.
 - c. User Account Deactivation and Termination
 - i) User accounts shall be deactivated or terminated promptly upon an individual's departure, job role change, or termination of employment.
 - ii) Account deactivation procedures should ensure the removal of user access to Company resources, including systems, applications, and data.
 - d. User Account Review
 - i) Regular reviews of user accounts and access rights shall be conducted to identify and address any inactive, unused, or unauthorized accounts.
 - ii) Account reviews should be performed at least annually or whenever there are significant changes in user roles or privileges.
4. **Access Control**
 - a. Authentication
 - i) User authentication mechanisms, such as passwords, passphrases, or multi-factor authentication (MFA), shall be implemented to verify user identities.
 - ii) Passwords and passphrases should adhere to a strong password policy (refer to the "Password Policy" for specific guidelines).

b. Authorization

- i. Access to Company resources shall be granted based on the principle of least privilege, ensuring that users have the minimum access required to perform their job functions.
- ii. Access authorization should be regularly reviewed and updated to reflect changes in user roles or responsibilities.

c. Role-Based Access Control (RBAC)

- i) RBAC principles should be applied to assign access rights based on predefined roles or job functions.
- ii) RBAC should simplify access management and ensure consistency in access permissions across system and applications.

d. Segregation of Duties (SoD)

- i) SoD principles shall be applied to separate conflicting roles or duties to prevent unauthorized access or fraudulent activities.
- ii) SoD conflicts should be identified, documented, and addressed during access provisioning and review processes.

e. Access Revocation

- i) Access rights shall be promptly revoked when no longer required, such as when a user changes job role or leaves the Company.
- ii) Revocation procedures should ensure the removal of user access to all relevant systems, applications, and data.

5. User Awareness and Training**a. Security Awareness Training**

- i) Users shall receive regular security awareness training on access control best practices, password hygiene, phishing awareness, and other relevant topics.
- ii) Training programs should emphasize the importance of protecting user credentials and the potential risks of unauthorized access.

b. Acceptable Use Policy

- i) Users shall be provided with an acceptable use policy that defines acceptable and prohibited activities related to user accounts and access to Company resources.
- ii) Users should be required to acknowledge and adhere to the acceptable use policy as a condition of accessing Company systems and data.

6. Policy Review and Compliance**a. Policy Review**

- i) This User Management and Access Control Policy shall be reviewed periodically, at least annually, or as deemed necessary, to ensure its relevance, effectiveness, and alignment with industry best practices. ii) Any updates or amendments to this policy shall be approved by senior management and communicated to all relevant parties.

b. Non-Compliance

- i) Failure to comply with this policy may result in disciplinary action, including but not limited to warnings, suspension, termination, or legal action, as deemed appropriate based on the severity of non-compliance.

By adhering to this User Management and Access Control Policy, **VT Capital Market Private Limited** aims to protect its resources, prevent unauthorized access, and maintain the confidentiality, integrity, and availability of sensitive information.

Policy Title: Business Continuity Planning and Response Management Policy

Effective Date: [25th Aug 2025]

1. Purpose The purpose of this policy is to establish guidelines and procedures for Business Continuity Planning (BCP) and Response Management within **VT Capital Market Pvt Ltd**. This policy aims to ensure the continuity of critical business operations, minimize disruptions, and facilitate effective response and recovery in the event of incidents or disasters.
2. Scope This policy applies to all employees, contractors, and third-party service providers who are involved in business operations, IT systems, and critical processes within the Company.
3. Business Continuity Planning
 - a. Risk Assessment and Business Impact Analysis (BIA)
 - i) Regular risk assessments and BIAs shall be conducted to identify potential threats, vulnerabilities, and the impact on critical business functions.
 - ii) Risk assessments and BIAs should be documented and used as a basis for developing the BCP.
 - b. Business Continuity Plan Development and Maintenance
 - i) A comprehensive BCP shall be developed, documenting strategies, procedures, and resources required to respond to and recover from potential incidents or disasters.
 - ii) The BCP should include incident response plans, recovery strategies, communication protocols, and roles and responsibilities of key personnel.
 - c. Plan Testing and Exercises
 - i) Regular testing and exercises of the BCP shall be conducted to evaluate its effectiveness and identify areas for improvement.
 - ii) Different types of tests, such as tabletop exercises and simulated scenarios, should be performed to validate the readiness of the BCP.
 - d. Plan Review and Updates
 - i) The BCP shall be reviewed periodically, at least annually, or as deemed necessary, to ensure its relevance, accuracy, and alignment with changing business needs and emerging threats.
 - ii) Updates to the BCP should be approved by senior management and communicated to all relevant stakeholders.
4. Incident Response and Management
 - a. Incident Identification and Classification
 - i) Incidents and disruptions to business operations shall be promptly identified, assessed, and classified based on severity and impact.
 - ii) Incident classification criteria should be defined to guide the appropriate response and allocation of resources.

b. Incident Response Team

- i) An incident response team shall be established, comprising individuals with defined roles and responsibilities for managing and responding to incidents.
- ii) The incident response team should be trained, equipped, and empowered to effectively handle incidents and mitigate their impact.

c. Incident Response Procedures

- i) Incident response procedures shall be developed and documented, outlining the steps to be followed in the event of an incident.
- ii) Procedures should cover incident assessment, containment, communication, mitigation, recovery, and post-incident analysis.

d. Communication and Notification

- i) Clear communication channels and protocols shall be established to facilitate effective incident notification and communication within the Company and with relevant stakeholders.
- ii) Communication plans should include contact lists, escalation procedures, and alternative communication methods during emergencies.

e. Incident Documentation and Reporting

- i) Incidents and their corresponding response activities shall be thoroughly documented, including incident details, actions taken, and lessons learned.
- ii) Incident reports should be generated and shared with appropriate management, enabling a comprehensive understanding of the incident and driving continuous improvement.

5. Policy Review and Compliance**a. Policy Review**

- i) This BCP and Response Management Policy shall be reviewed periodically, at least annually, or as deemed necessary, to ensure its relevance, effectiveness, and alignment with industry best practices.
- ii) Any updates or amendments to this policy shall be approved by senior management and communicated to all relevant parties.

b. Non-Compliance

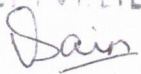
- i) Failure to comply with this policy may result in disciplinary action, including but not limited to warnings, suspension, termination, or legal action, as deemed appropriate based on the severity of non-compliance.

By adhering to this Business Continuity Planning and Response Management Policy, **VT Capital Market Pvt Ltd** aims to establish a proactive approach to minimize business disruptions, ensure the safety and well-being of employees, and protect the Company's reputation and critical operations during incidents or disasters.

Policy Title: Order Level Checks PolicyEffective Date: [25th Aug 2025]

1. Purpose The purpose of this policy is to establish guidelines and procedures for conducting comprehensive checks at the order level within VT Capital Market Private Limited ("the Company"). This policy aims to ensure the accuracy, completeness, and compliance of orders placed by clients, minimizing errors, discrepancies, and potential risks associated with order processing.
 2. Scope This policy applies to all employees, contractors, and any individuals involved in the process of receiving, reviewing, and executing orders within the Company.
- 3. Order Verification and Validation**
- a. Order Receipt and Acknowledgment
 - i) Orders received from clients shall be promptly acknowledged, ensuring proper documentation and record keeping.
 - ii) Acknowledgment procedures should include confirmation of order details, client identification, and validation of authorized individuals placing the order.
 - b. Order Verification
 - i) Order details, including security, quantity, price, and any specific instructions, shall be thoroughly verified against client records and trading requirements.
 - ii) Order verification should include cross-referencing with relevant systems, validating account balances, and ensuring compliance with regulatory requirements.
 - c. Compliance Checks
 - i) Orders shall be subjected to compliance checks to ensure adherence to applicable laws, regulations, and internal policies.
 - ii) Compliance checks should cover areas such as insider trading, market manipulation, client suitability, and any other regulatory restrictions.
 - d. Risk Assessment
 - i) Orders shall be assessed for potential risks, such as unusual trading patterns, high-risk securities, or orders from high-risk clients.
 - ii) Risk assessment procedures should consider established risk models, historical data, and any red flags identified during order verification.
- 4. Order Execution and Monitoring**
- a. Best Execution
 - i) Orders shall be executed in compliance with the Company's best execution policy, ensuring the timely and fair execution of client orders.
 - ii) Best execution practices should consider factors such as price, liquidity, speed, and likelihood of execution.

VT CAPITAL MARKET PVT. LTD.


Director

b. Order Monitoring

- i) Ongoing monitoring of order execution shall be conducted to ensure timely and accurate processing, addressing any exceptions or discrepancies promptly.
- ii) Monitoring procedures should include order status tracking, confirmation of executed trades, and resolution of any failed or rejected orders.

c. Trade Reconciliation

- i) Executed trades shall be reconciled with the corresponding orders to verify accuracy, identify any trade breaks or discrepancies, and ensure proper trade settlement.
- ii) Trade reconciliation processes should be performed promptly, involving collaboration between the relevant departments, such as trading, operations, and settlement teams.

5. Documentation and Record Keeping**a. Order Documentation**

- i) Comprehensive documentation of order details, including client instructions, order confirmations, and any modifications, shall be maintained.
- ii) Order documentation should be securely stored and easily retrievable for audit purposes.

b. Record Retention

- i) Order records and related documentation shall be retained in accordance with applicable laws, regulations, and the Company's record retention policy.
- ii) Record retention procedures should ensure the confidentiality, integrity, and accessibility of order-related documents.

6. Policy Review and Compliance**a. Policy Review**

- i) This Order Level Checks Policy shall be reviewed periodically, at least annually, or as deemed necessary, to ensure its relevance, effectiveness, and alignment with industry best practices.
- ii) Any updates or amendments to this policy shall be approved by senior management and communicated to all relevant parties.

b. Non-Compliance

- i) Failure to comply with this policy may result in disciplinary action, including but not limited to warnings, suspension, termination, or legal action, as deemed appropriate based on the severity of non-compliance.

By adhering to this Order Level Checks Policy, **VT Capital Market Private Limited** aims to ensure the accuracy, integrity, and compliance of client orders throughout the order processing lifecycle. This policy promotes efficient order execution, risk mitigation, and adherence to regulatory requirements, safeguarding the interests of clients and maintaining the Company's reputation for excellence in order handling.

Policy Title: Policy For Disposal of Storage Media**Effective Date : [25th Aug 2025]**

1. **Purpose** The purpose of this policy is to establish guidelines and procedures for conducting comprehensive checks at the order level within VT Capital Market Private Limited ("the Company"). This policy aims to ensure the accuracy, completeness, and compliance of orders placed by clients, minimizing errors, discrepancies, and potential risks associated with order processing.
2. **Scope** this policy covers all situations involving the disposal of removable storage media. In our company must ensure that all removable storage media are cleaned before being disposal of.

3 Responsibilities

It is the responsibility of our company authorized IT person to manage the secure disposal of all storage media that is no longer required, according to this policy.

All owners of removable storage media are responsible for disposing of removable storage media according to this policy.

4 Procedure.

- i) Hard disks must be formatted and cleaned of all data and software before being reused or disposed of.
- ii) Hard disks must be cleaned and verified by an independent and certified provider.
- iii) Removable storage media devices that contain confidential information must be destroyed only after a risk assessment has been carried out and must never be reused.
- iv) Removable storage media devices that contain confidential information must be subjected to a risk assessment before they are sent for repair in order to establish whether they ought to be repaired or replaced.
- v) All media must be disposed of according to the legal and regulatory requirements for the disposal of computer equipment, via an independent and certified provider.
- vi) Documents that contain confidential and restricted information should be shredded by their owners prior to being destroyed. Shredders are located in office. The shredded waste must be removed by an approved service provider.

5 Storage Media Guidelines

Disposal of Inoperable or Damaged Media All electronic storage media must be destroyed when it has reached the end of its useful life and/or when other sanitizing methods are not effective, provided the destruction does not conflict with data retention policies or other regulatory requirements (e.g., electronic discovery).

6 Disposal of Inoperable or Damaged Media

All electronic storage media must be destroyed when it has reached the end of its useful life and/or when other sanitizing methods are not effective, provided the destruction does not conflict with data retention policies or other regulatory requirements (e.g., electronic discovery).

Policy Title: Disposal and Data Retention policy

Effective Date: [25th Aug 2025]

Creating a Disposal and Data Retention Policy for cybersecurity is critical to ensure that sensitive data is managed responsibly within VT Capital Market Pvt Ltd Here's a comprehensive guide to establishing such a policy:

1. Purpose and Scope

- **Purpose:** Define the goals of the policy, emphasizing the importance of protecting sensitive data and ensuring compliance with relevant regulations.
- **Scope:** Specify the types of data covered (e.g., personal data, financial data, health information) and the systems, devices, and personnel involved.

2. Data Classification

- **Classification Levels:** Establish data classification levels (e.g., Public, Internal, Confidential, Restricted) based on the sensitivity and impact of data exposure.
- **Handling Requirements:** Outline specific handling requirements for each classification level.

3. Data Retention Schedule

- **Retention Periods:** Define how long different types of data should be retained based on legal, regulatory, and business requirements.
- **Review Process:** Establish a regular review process to ensure retention periods remain appropriate and compliant with changing regulations.

4. Data Storage and Security

- **Storage Locations:** Identify approved storage locations for different data types, including on-premises servers, cloud services, and physical archives.

- **Security Measures:** Detail the security measures required to protect data at each classification level, such as encryption, access controls, and audit logging.

5. Data Disposal Procedures

- **Methods of Disposal:** Specify approved methods for data disposal (e.g., shredding, degaussing, secure erasure) tailored to the type and sensitivity of the data.
- **Documentation:** Require documentation of the disposal process, including the date, method, and personnel involved.

6. Roles and Responsibilities

- **Data Owners:** Define the responsibilities of data owners in managing the lifecycle of their data, including classification, retention, and disposal.
- **IT and Security Teams:** Outline the roles of IT and security teams in implementing and enforcing the policy.
- **Compliance Officer:** Assign a compliance officer to oversee adherence to the policy and conduct periodic audits.

7. Legal and Regulatory Compliance

- **Relevant Laws and Regulations:** List the specific laws and regulations that govern data retention and disposal (e.g., GDPR, HIPAA, CCPA).
- **Compliance Monitoring:** Describe the processes for monitoring compliance with these regulations.

8. Training and Awareness

- **Employee Training:** Implement regular training programs to ensure employees understand their roles in data protection and are aware of the policy.
- **Awareness Campaigns:** Conduct awareness campaigns to highlight the importance of data retention and disposal.

9. Incident Response

- **Data Breaches:** Detail the procedures for responding to data breaches, including notification requirements and mitigation steps.
- **Non-compliance:** Define the consequences and corrective actions for non-compliance with the policy.

10. Policy Review and Updates

- **Periodic Review:** Establish a schedule for periodic review and updating of the policy to reflect new threats, technologies, and regulatory changes.
- **Feedback Mechanism:** Provide a mechanism for employees to suggest improvements to the policy.

Example of a Data Retention and Disposal Schedule

Data Type	Retention Period	Disposal Method
Financial Records	10 years	Shredding
Employee Records	Duration of Employment + 5 years	Secure Erasure
Audit Logs	3 year	Secure Erasure

Implementation Steps

1. **Policy Development:** Draft the policy with input from legal, compliance, IT, and business units.
2. **Approval:** Obtain approval from senior management and relevant stakeholders.
3. **Communication:** Communicate the policy to all employees and provide necessary training.
4. **Enforcement:** Implement technical and administrative controls to enforce the policy.
5. **Monitoring and Auditing:** Regularly monitor compliance and conduct audits to ensure adherence to the policy.
6. **Continuous Improvement:** Use audit results and feedback to continuously improve the policy.

By adhering these guidelines, **VT Capital Market Pvt Ltd** can create a robust Disposal and Data Retention policy that protects sensitive data, ensures compliance, and mitigates risks associated with data breaches and improper data handling.

Policy Title: Data Leakage Policy

Effective Date: [25th Aug 2025]

1. Purpose

The purpose of this policy is to protect the confidentiality, integrity, and availability of sensitive information by preventing unauthorized data leakage from the organization's systems and networks.

2. Scope

This policy applies to all employees, contractors, and third-party users who have access to the organization's information systems, networks, and data.

3. Definitions

- **Data Leakage:** Unauthorized transmission of data from within an organization to an external destination or recipient.
- **Sensitive Information:** Any data that could cause harm to the organization or its stakeholders if disclosed, including personal data, financial information, intellectual property, and proprietary information.

4. Policy Statements

4.1 Data Classification

All data must be classified according to its sensitivity level. The classification categories are:

- Public
- Internal
- Confidential
- Restricted

4.2 Access Control

Access to sensitive information must be restricted based on the principle of least privilege. Only authorized personnel with a legitimate need to know shall have access to such data.

4.3 Data Transmission

Sensitive information must be transmitted using secure channels, such as encrypted email, VPNs, or secure file transfer protocols.

4.4 Data Storage

Sensitive information must be stored securely, with appropriate encryption measures in place both at rest and in transit.

4.5 Monitoring and Detection

The organization shall implement monitoring and detection systems to identify potential data leakage incidents. This includes network monitoring, data loss prevention (DLP) tools, and regular audits.

4.6 Employee Training

All employees must receive regular training on data leakage prevention, including recognizing potential threats and understanding their responsibilities under this policy.

4.7 Incident Response

In the event of a suspected data leakage incident, the following steps must be taken:

- Immediate containment of the incident
- Investigation to determine the cause and extent of the leak
- Notification of affected parties, if applicable
- Remediation to prevent future incidents

5. Roles and Responsibilities

- **IT Department:** Responsible for implementing and maintaining technical measures to prevent data leakage.
- **Security Team:** Responsible for monitoring and responding to data leakage incidents.
- **Employees:** Responsible for adhering to this policy and reporting any suspected data leakage incidents.

6. Compliance

Failure to comply with this policy may result in disciplinary action, up to and including termination of employment. Legal action may also be taken in cases of severe breaches.

7. Review and Revision

This policy shall be reviewed annually and updated as necessary to reflect changes in technology, regulatory requirements, and organizational needs.

Appendices

A. Data Classification Guidelines

- **Public:** Information that is intended for public use and disclosure poses no risk to the organization.
- **Internal:** Information that is intended for internal use only and is not for public disclosure.
- **Confidential:** Sensitive information that requires protection from unauthorized disclosure.
- **Restricted:** Highly sensitive information that requires the highest level of protection.

B. Incident Response Plan

1. **Identification:** Detect and identify the data leakage incident.
2. **Containment:** Implement measures to contain the leak.
3. **Eradication:** Remove the root cause of the leak.
4. **Recovery:** Restore affected systems and data.
5. **Lessons Learned:** Conduct a post-incident review to improve future responses.

This policy provides a framework for protecting sensitive information and mitigating the risks associated with data leakage. Implementing and adhering to these guidelines can help safeguard VT Capital Market Pvt Ltd data and maintain trust with stakeholders.

Policy Title: BYOD(Bring Your Own Device)Policy

Effective Date: [25th Aug 2025]

1. Purpose

The purpose of this policy is to establish guidelines for the use of personally owned devices by employees to access company systems, networks, and data, ensuring the security and integrity of the organization's information.

2. Scope

This policy applies to all employees, contractors, and third-party users who wish to use their personal devices (smartphones, tablets, laptops, etc.) to access the organization's resources.

3. Definitions

- **BYOD:** Bring Your Own Device, refers to the policy of permitting employees to use their personal devices for work purposes.
- **Device:** Any personally owned electronic equipment such as smartphones, tablets, laptops, and other portable computing devices.

4. Policy Statements

4.1 Device Enrollment

- Employees must enroll their devices with the IT department before accessing company systems.
- Devices must meet the organization's security standards and requirements.

4.2 Security Requirements

- All devices must have up-to-date antivirus and anti-malware software installed.
- Devices must be configured to use strong passwords or biometric authentication.
- Encryption must be enabled on all devices to protect data at rest.
- Employees must install and regularly update any required security software or apps as directed by the IT department.

4.3 Access Control

- Access to company resources will be limited based on the role and responsibilities of the user.
- VPNs or other secure connection methods must be used to access company networks remotely.
- Devices must automatically lock after a period of inactivity.

4.4 Data Management

- Employees must not store sensitive company data on their personal devices unless necessary and authorized.
- If sensitive data must be stored, it should be done in an encrypted and secure manner.
- Employees must back up data regularly in accordance with company policies.

4.5 Monitoring and Compliance

- The organization reserves the right to monitor devices for compliance with this policy.
- IT may conduct regular audits to ensure devices adhere to security requirements.
- Employees must cooperate with any security incident investigations involving their personal devices.

4.6 Incident Reporting

- Any loss, theft, or breach of a personal device that has access to company resources must be reported to the IT department immediately.
- Employees must assist with the investigation and remediation of any data breach incidents.

4.7 Usage Restrictions

- Personal devices must not be used to engage in illegal activities or conduct that violates company policies.
- The use of unauthorized applications or software that pose security risks is prohibited.

4.8 Employee Responsibilities

- Employees are responsible for maintaining the physical and cyber security of their personal devices.
- Employees must ensure their devices are used in accordance with this policy at all times.
- Employees must not share their devices with unauthorized individuals while they are connected to the company network.

5. Roles and Responsibilities

- **Employees:** Ensure compliance with the BYOD policy and report any incidents.
- **IT Department:** Manage device enrollment, enforce security requirements, and respond to incidents.
- **Security Team:** Monitor device usage and investigate security breaches.

6. Compliance

Failure to comply with this policy may result in disciplinary action, up to and including termination of employment. Non-compliance may also lead to loss of BYOD privileges.

7. Review and Revision

This policy shall be reviewed annually and updated as necessary to reflect changes in technology, regulatory requirements, and organizational needs.

Appendices

A. Acceptable Use Guidelines

- Personal devices must only be used for work-related activities during working hours.
- Employees must adhere to company policies on acceptable use of IT resources.

B. Device Security Checklist

- Ensure the device is running the latest operating system version.
- Install and update antivirus software regularly.
- Enable encryption and automatic locking.
- Use strong passwords or biometric authentication.

Implementing and adhering to this BYOD policy helps ensure that personal devices used for work purposes do not compromise the security of the organization's data and systems.

Policy Title : Standard Operating Procedure (SOP) for handling cyber security incidents of intermediaries.

Effective Date: [25th Aug 2025]

1. Introduction

This SOP outlines the procedures and steps to be followed for managing and responding to cybersecurity incidents involving intermediaries such as ISPs, cloud service providers, and other digital platforms. The primary goal is to ensure a coordinated, efficient, and effective response to minimize impact and prevent recurrence.

2. Scope

This procedure applies to all intermediaries that provide services involving data processing, storage, or transmission. It covers the identification, response, mitigation, reporting, and post-incident review of cybersecurity incidents.

3. Definitions

- **Cybersecurity Incident:** Any event that compromises the confidentiality, integrity, or availability of information or information systems.

- **Intermediary:** Entities that facilitate the use of the internet or digital platforms, such as ISPs, hosting services, and content delivery networks.

4. Roles and Responsibilities

- **Incident Response Team (IRT):** The primary team responsible for handling the incident.
- **IT Department:** Supports the IRT with technical expertise and resources.
- **Legal and Compliance Team:** Ensures all legal and regulatory obligations are met.
- **Communications Team:** Manages internal and external communication related to the incident.
- **Senior Management:** Provides oversight and strategic decisions during major incidents.

5. Incident Response Phases

1. Preparation

- Establish and train the Incident Response Team.
- Develop and maintain an Incident Response Plan.
- Ensure necessary tools and resources are available.

2. Identification

- Detect and confirm the incident using monitoring tools and alerts.
- Gather initial information and determine the scope and impact.

3. Containment

- Short-term: Implement measures to limit the immediate impact.
- Long-term: Implement measures to prevent further spread and address vulnerabilities.

4. Eradication

- Identify and remove the root cause of the incident.
- Ensure all malicious artifacts are eliminated.

5. Recovery

- Restore affected systems and services to normal operation.
- Verify systems are functioning correctly and securely.

6. Lessons Learned

- Conduct a post-incident review to analyze the response and identify improvements.
- Update the Incident Response Plan and training materials accordingly.

6. Detailed Procedures

6.1 Preparation

- Develop and document the Incident Response Plan.
- Conduct regular training and simulations.
- Maintain updated contact lists and escalation procedures.
- Ensure all systems are patched and up-to-date with security measures.

6.2 Identification

- Monitor for unusual activity or alerts from intrusion detection systems.
- Log all incident-related information.
- Notify the Incident Response Team immediately upon suspicion or confirmation of an incident.

6.3 Containment

- Disconnect affected systems from the network if necessary.

- Apply firewall rules or access controls to isolate the threat.
- Implement temporary fixes or workarounds to prevent escalation.

6.4 Eradication

- Perform a thorough investigation to identify all affected components.
- Remove malware, unauthorized access points, and other malicious artifacts.
- Verify the removal of all threats before proceeding to recovery.

6.5 Recovery

- Restore data from clean backups.
- Rebuild or reinstall affected systems as needed.
- Monitor systems closely for any signs of lingering issues.
- Communicate with stakeholders about the status and resolution of the incident.

6.6 Lessons Learned

- Gather detailed documentation of the incident and response.
- Hold a meeting with all involved parties to discuss what happened and why.
- Identify strengths and weaknesses in the response.
- Update policies, procedures, and training based on the findings.

7. Reporting

- Report the incident to relevant regulatory bodies as required.
- Document the incident thoroughly, including timelines, actions taken, and outcomes.
- Share relevant information with other intermediaries to help prevent similar incidents.

8. Communication

- Develop a communication plan for internal and external stakeholders.
- Provide regular updates to affected customers and partners.
- Ensure all communications are clear, transparent, and accurate.

9. Compliance and Legal Considerations

- Ensure all actions comply with relevant laws and regulations.
- Consult with legal counsel as needed throughout the incident response process.
- Preserve evidence for potential legal proceedings.

10. Continuous Improvement

- Regularly review and update the Incident Response Plan.
- Incorporate lessons learned from incidents and simulations.
- Stay informed about new threats and best practices in cybersecurity.

This SOP provides a structured approach to managing cybersecurity incidents, ensuring that intermediaries can effectively respond to and recover from incidents while minimizing damage and preventing future occurrences.

Policy Title : Work From Home (WFH) Environment PolicyEffective Date: [25th Aug 2025]**1. Purpose**

This policy outlines the guidelines and expectations for employees working from home (WFH) to ensure productivity, security, and compliance. It aims to provide a clear framework for remote work while maintaining the quality of work and protecting company assets.

2. Scope

This policy applies to all employees who are approved to work from home either full-time or part-time.

3. Eligibility

- Employees must obtain approval from their direct supervisor and HR to participate in the WFH program.
- Roles that require physical presence, such as certain operational and administrative positions, may not be eligible for WFH.

4. Work Environment Requirements

Employees must ensure their home office environment is conducive to productive work. This includes:

- A quiet, private workspace free from distractions.
- Reliable internet connection.
- Necessary hardware and software to perform job duties (e.g., computer, phone, VPN access).
- Adequate security measures to protect company data (e.g., locked cabinets, secure Wi-Fi).

5. Work Hours and Availability

- Employees are expected to maintain regular work hours as agreed upon with their supervisor.
- Employees should be accessible via phone, email, and other communication tools during work hours.
- Any changes to work hours or availability must be communicated and approved in advance.

6. Productivity and Performance

- Employees must meet the same performance and productivity standards as those working in the office.
- Regular check-ins with supervisors to discuss progress and any challenges.
- Use of productivity tools and software as required by the company.

7. Communication

- Regular communication with team members and supervisors via email, phone, or video conferencing.
- Participation in all mandatory meetings and calls.
- Clear and timely responses to communications.

8. Data Security and Confidentiality

- Adherence to company data security policies and procedures.
- Use of company-approved tools for storing and sharing work-related information.

- Immediate reporting of any security incidents or breaches to the IT department.

9. Health and Safety

- Employees must ensure their home workspace complies with health and safety regulations.
- Proper ergonomic setup to prevent strain and injury.
- Adherence to regular breaks and movement to maintain physical well-being.

10. Equipment and Resources

- The company may provide necessary equipment such as laptops, monitors, and software licenses.
- Employees are responsible for the care and maintenance of company-provided equipment.
- Any issues with equipment must be reported to the IT department promptly.

11. Expense Reimbursement

- The company may reimburse certain expenses related to WFH (e.g., internet, phone bills) as per the reimbursement policy.
- Pre-approval from the finance department may be required for certain expenses.

12. Compliance and Monitoring

- Regular audits and monitoring to ensure compliance with WFH policies.
- Employees must cooperate with any compliance checks or audits.
- Non-compliance with the WFH policy may result in disciplinary action, up to and including termination.

13. Review and Updates

- This policy will be reviewed periodically and updated as needed.
- Employees will be informed of any changes to the policy.

This WFH policy aims to support employees in maintaining a productive and secure work environment while working remotely. It establishes clear expectations and guidelines to ensure the success of remote work arrangements.

After the pandemic, VT Capital Market Private Limited has given strict instructions that no employee should work from home.

Policy Title : Data Encryption PolicyEffective Date: [25th Aug 2025]**Policy and statement**

- **Encrypt Sensitive Data**
 - Always encrypt confidential, personal, financial, or regulated data.
 - Apply encryption to data **at rest** (stored) and **in transit** (sent over networks).
- **Use Strong Encryption Standards**
 - Use only approved algorithms like **AES-256** for storage and **TLS 1.2 or higher** for transmission.
 - Avoid outdated or weak encryption (e.g., DES, SSL, or MD5).
- **Secure Encryption Keys**
 - Store keys in a secure **Key Management System (KMS)**.
 - Never hard-code or email encryption keys.
 - Rotate keys regularly and immediately if compromised.
- **Protect End-User Devices**
 - Enable full disk encryption on laptops, USBs, and mobile devices.
 - Require strong passwords and auto-lock features on devices.
- **Encrypt Backups**
 - Ensure all backup files and archives are encrypted, both onsite and in the cloud.
- **Verify Cloud Provider Compliance**
 - Use cloud services that offer built-in encryption and comply with security standards (e.g., ISO 27001, GDPR).
- **Avoid Sending Sensitive Data via Unencrypted Channels**
 - Do **not** send passwords, credit card numbers, or personal data over unprotected email or messaging apps.
- **Educate Staff**
 - Train employees on when and how to encrypt data.
 - Emphasize the importance of reporting lost devices or suspicious activity.

- **Monitor and Audit**

- Regularly audit systems for compliance with encryption policies.
- Use tools to monitor encryption status and key access.

Policy Title: Patch management procedure

Effective Date: [25th Aug 2025]

1. Scope

Applies to our organizational hardware, software, operating systems, applications, and network devices.

2. Patch Identification

- Monitor vendor notifications and vulnerability databases.
- Use automated tools to detect required patches.

3. Assessment & Testing

- Evaluate patch criticality and system relevance.
- Test patches in a controlled environment to ensure compatibility and stability.

4. Approval Process

- Critical patches may be fast-tracked.
- Standard patches require stakeholder review and approval.

5. Deployment

- Schedule during maintenance windows.
- Use patch management tools for efficient deployment.
- Ensure rollback plans are in place.

6. Verification

- Confirm successful patch application.
- Monitor systems for post-patch issues.

7. Documentation & Reporting

- Maintain logs of patches applied, systems affected, and any issues encountered.
- Report regularly to IT and security leadership.

8. Frequency

- Critical patches: within 24–72 hours.
- Routine patches: monthly or as needed.

9. Compliance

- Align with regulatory standards (e.g., NIST, ISO 27001, HIPAA).
- Conduct regular audits and reviews.

10. Exceptions

- Must be documented and approved.
- Include mitigation steps if patches cannot be applied.

Policy Title: Event log and monitoring Procedure

Effective Date: [25th Aug 2025]

1. **Scope**
Applies to all critical systems, applications, servers, and network devices within the organization.
2. **Log Sources**
 - Operating systems (Windows, Linux)
 - Applications and databases
 - Firewalls, IDS/IPS, routers
 - Cloud services and endpoint protection tools
3. **Event Types Monitored**
 - Security events (e.g., login failures, access violations)
 - System events (e.g., service failures, resource usage)
 - Application errors and warnings
 - Audit logs for compliance
4. **Log Collection & Storage**
 - Centralized logging using tools (e.g., SIEM, syslog servers)
 - Secure, tamper-proof storage with defined retention periods
 - Retention aligned with policy and compliance (e.g., 90 days to 1 year)
5. **Monitoring & Alerting**
 - Real-time or near real-time monitoring
 - Automatic alerts for suspicious or critical events
 - Prioritized alert levels (info, warning, critical)
6. **Analysis & Correlation**
 - Correlate events across systems to identify threats
 - Use automated tools for anomaly detection
 - Manual review for high-risk or complex issues
7. **Incident Response Integration**
 - Escalate alerts to incident response teams
 - Trigger predefined response procedures
8. **Review & Reporting**
 - Regular log review (daily, weekly, monthly)
 - Generate reports for audits and performance reviews
9. **Access Control & Integrity**
 - Restrict log access to authorized personnel only
 - Ensure logs are protected from unauthorized modification
10. **Compliance & Audit Support**
 - As need VT Capital Market Pvt Ltd Provide logs during audits or investigations.

VT CAPITAL MARKET PVT. LTD.

Sain
Director

Policy Title: Restoration Mechanism PolicyEffective Date: [25th Aug 2025]

1. Purpose To ensure that important data can be restored quickly and completely after accidental deletion, hardware failure, ransomware, or disaster.
2. Scope Applies to all company data: files, databases, emails, applications, laptops, servers, and cloud service
3. Simple Rule Everyone Follows: 2-1 Backup Rule
 - 2 different types of storage (e.g., server + external drive)
 - 1 copy kept offline or off-site (safe from ransomware and local disasters)

4. Minimum Requirements (What Must Be Done)

Data Type	Backup Frequency	Retention	Restoration Target
Critical data (customer DB, financials, contracts)	Daily	30 days + 1 yearly	Restore within 4–8 hours
Important files (shared drives, projects)	Daily or weekly	30 days	Restore within 1 business day
Laptops / user devices	Daily (automated)	14–30 days	User can self-restore within 4 hours by IT

5. Required Protection Methods

- Backups must be automated (no manual copying)
- At least one backup must be offline or immutable (cannot be deleted by ransomware)
- Backups must be encrypted
- Cloud backups must have versioning or recycle bin enabled
- Test restoration at least once every 6 months

6. Approved Simple Tools (choose one or more)

- Sql Database: Database Backup by SQL in automated ,
- Important file like doc.xls and pdf

7. Who Can Restore Data

- Normal files: Users can restore from recycle bin or self-service portal
- Major recovery (disaster/ransomware): Only IT team or designated admin
- All major restores must be logged

8. Testing

- Every 6 months, IT must successfully restore at least one full system or critical folder from backup
- Result must be documented (date, what was restored, time taken)

9. Ransomware Rule (Very Important) Never connect all backups to the network at the same time. Always keep one copy completely offline (external drive unplugged or cloud with Object Lock

10. Policy Review This policy will be reviewed and updated once per year or after any major incident. Approved

by: Manoj Prasad (IT Manager)

Date: 25th Aug 2025

Policy Title: Misuse Prevention PolicyEffective Date: [25th Aug 2025]

- Here's a concise, practical example of an effective misuse prevention policy (the kind many responsible AI companies, developers, or organizations adopt as a starting point): Misuse Prevention Policy (example)

1) Prohibited Activities

Users may not use the system to:

- Directly facilitate or commit illegal acts (e.g., fraud, trafficking, terrorism, child sexual abuse material, scams, etc.).
- Create or distribute non-consensual intimate imagery .
- Provide instructions for building weapons of mass destruction or highly regulated restricted item (e.g., biological agents, nuclear weapons).
- Impersonate authorities or forge official documents in a way that could cause serious real-world harm.
- Conduct large-scale disinformation campaigns intended to interfere with democratic elections or public health.

2) High-Risk Activities (restricted or monitored)

- Giving specific, step-by-step instructions for serious self-harm or suicide.
- Providing detailed guidance on committing serious crimes (e.g., how to manufacture illegal drug at scale, how to hack critical infrastructure).
- Generating output that targets protected groups with credible threats or coordinated harassment.

3) Allowed (with common-sense limits)

- Hypothetical discussions, fiction, research, journalism, or satire — even on sensitive topics.
- General knowledge (chemistry, history, lock picking theory, etc.) that is publicly available.
- Adult sexual content between consenting adults (text or imagery) as long as it doesn't violate #1 or #2.

4) Enforcement Approach

- Hard refusals for clear violations of prohibited categories.
- Warnings or limited answers for edge cases.
- Logging and review of repeated attempts to bypass safeguards.
- Continuous updating of filters based on new abuse patterns.

This kind of policy is “basic” because it focuses on the highest-harm, lowest-free-speech-impact Cases first. It avoids over-blocking legitimate use (academic research, creative writing, security Testing, etc.) while still protecting society from the worst abuses.