Netweb

TECHNOLOGIES

IT SECURITY POLICY

1. PURPOSE

Netweb Technologies India Limited ("NTIL") is committed to securing its digital infrastructure, information systems, and sensitive data from an increasingly complex landscape of IT Security threats. This IT Security Policy establishes a comprehensive framework of guidelines, principles, and best practices to ensure the confidentiality, integrity, and availability of NTIL's digital assets and IT resources.

This policy outlines NTIL's strategic approach to IT Security, serving as the foundation for detailed operational policies in areas such as network security, cloud computing, remote access, endpoint protection, and data management. It integrates both preventive and responsive security measures, aiming to reduce the risk of cyber incidents and unauthorized access while enhancing user awareness and compliance.

Recognizing that no single policy can eliminate cyber risks entirely, this framework is designed to significantly mitigate vulnerabilities and strengthen NTIL's ability to detect, respond to, and recover from security breaches. It establishes a culture of security awareness and proactive governance that supports business continuity, legal compliance, and stakeholder confidence.

The primary objectives of this IT Security Policy is to:

- Safeguard NTIL's information technology resources from misuse, damage, or theft.
- Prevent unauthorized access to corporate data and systems.
- Maintain data integrity and operational continuity.
- Ensure compliance with applicable data protection laws and industry regulations.
- Define roles, responsibilities, and response mechanisms for managing IT Security risks

2. SCOPE

This Data Security Policy applies to all forms of sensitive information, including but not limited to customer data, personal data (employee and client-related), proprietary business data, any classified or confidential information as defined by NTIL.

The policy covers all infrastructure that stores, processes, or transmits sensitive information, including servers, databases, and storage systems, IT systems, applications, and cloud platforms, devices used for email, internet access, collaboration, and work-related functions.

This policy applies to:

- All personnel, including full-time and part-time employees, contractors, consultants, interns, and third-party vendors who access or manage NTIL's information systems and resources.
- All IT assets, including company-managed hardware, software, communication systems, networks, mobile devices, and applications—whether hosted on-premises or in the cloud.

- All access points, whether internal or remote, ensuring comprehensive compliance across physical and digital environments.

3. **NEED FOR THE POLICY**

This policy is essential for establishing a consistent, organization-wide approach to IT Security and data protection. The key drivers include:

- **Establishes a Framework for Security Controls**
  This policy acts as a strategic guideline for implementing appropriate security measures across the organization. While it does not mandate specific technical configurations, it reflects senior management's vision and expectations for IT Security. It provides direction to IT and security teams, who are responsible for translating these principles into concrete, technically sound safeguards in line with industry standards and legal requirements.
- **Defines Clear Security Expectations**
  In the absence of clear policies, employees may adopt inconsistent or insecure practices when handling sensitive information or using IT systems. This policy mitigates that risk by outlining standardized security expectations, roles, and responsibilities. It ensures all employees are aware of appropriate behaviours, restrictions, and procedures, thereby reducing the likelihood of human error and information security incidents.
- **Enhances Operational Efficiency and Business Alignment**
  A structured security policy contributes to operational efficiency by streamlining processes, reducing duplication of effort, and promoting consistent enforcement of security protocols. It also defines a formal mechanism for managing policy exceptions, allowing deviations to be documented, justified, and monitored. By aligning security controls with business goals, operational workflows, and organizational culture, the policy supports secure and sustainable business growth.

4. **INFORMATION SECURITY**

NTIL recognizes that ensuring the confidentiality, integrity, and availability of its information assets is essential for protecting sensitive data and maintaining uninterrupted business operations. The company is committed to upholding the highest standards of information security by adopting the following key measures:

- **Robust Security Controls:** NTIL will implement and maintain comprehensive security controls and procedures to safeguard all information assets against unauthorized access, disclosure, alteration, or destruction. These controls will be regularly reviewed and updated to address evolving security threats and technological advancements.
- **Security Awareness and Training:** To foster a culture of security-conscious behaviour, all employees, contractors, and third-party service providers will receive regular information security awareness training. This training will cover best practices, emerging threats, and individual responsibilities for protecting organizational data and systems.
- **Regulatory and Legal Compliance:** NTIL shall ensure strict adherence to applicable legal, regulatory, and contractual requirements, including but not limited to the Information Technology Act, 2000, the Digital Personal Data Protection Act, 2023, and industry-specific compliance standards.

Non-compliance risks will be actively managed and mitigated through proactive monitoring and internal controls.

- **Continuous Monitoring and Improvement:** Information security will be continuously assessed through proactive risk identification, threat detection, vulnerability scanning, and incident response mechanisms. NTIL is committed to enhancing its security posture through ongoing evaluation, feedback, and the adoption of emerging technologies and frameworks.

5. **DATA SECURITY**

Data security at NTIL encompasses a comprehensive suite of practices, technologies, and governance mechanisms aimed at protecting digital assets from unauthorized access, loss, corruption, or theft throughout the data lifecycle.

Key Components of Data Security

- **Physical Security:** Data centers, servers, and storage devices must be housed in secure, access-controlled environments to prevent physical tampering or theft. Environmental safeguards (e.g., fire suppression systems, temperature control) shall be in place to protect hardware integrity.
- **Administrative Controls:** Access to sensitive data will be strictly controlled based on roles and responsibilities. User privileges will be defined and enforced through clearly established procedures, including periodic access reviews and segregation of duties.
- **Logical Security Measures:** Robust logical controls such as encryption (in transit and at rest), multi-factor authentication (MFA), secure application design, and firewalls shall be used to prevent unauthorized access and ensure data integrity and confidentiality.
- **Policy and Governance:** Formal data management and retention policies shall govern the classification, handling, storage, and disposal of data. These policies will be aligned with applicable legal and regulatory frameworks to ensure compliance and accountability.
- **Contractual Agreements:** Vendor contracts will include provisions for data protection, security standards, and incident reporting.

By implementing an integrated data security framework, NTIL commits to protecting its business, employees, clients, and stakeholders from the repercussions of data loss, breaches, or misuse.

6. **Technical Safeguards and Risk Mitigation Measures**

a) **Encryption**: Encryption is a critical component of Netweb Technologies India Limited's (NTIL) data security framework, designed to protect the confidentiality and integrity of sensitive information both at rest and in transit. By transforming readable data (plaintext) into an unreadable format (ciphertext) using cryptographic algorithms and encryption keys, NTIL ensures that only authorized users can access protected information. Encryption is considered a final and non-negotiable layer of defence in NTIL’s IT Security strategy, helping mitigate the risks of data breaches, cyberattacks, and insider threats.

b) **Data erasure:** Data erasure is a critical process employed by NTIL to securely and permanently remove data from storage devices, ensuring that no residual data can be recovered or misused. It goes beyond basic deletion or formatting by using specialized software to overwrite data multiple times and verify its complete removal. Secure data erasure helps NTIL reduce the risk of data leaks, ensure privacy compliance, and uphold trust among stakeholders.

c) **Data masking:** Data masking is a critical security practice implemented by NTIL to safeguard sensitive data such as Personally Identifiable Information (PII) while enabling legitimate business operations like software development, testing, training, and analytics. Data masking ensures that sensitive information remains protected in non-production environments, allowing employees and third parties to work with realistic datasets without compromising data privacy or violating compliance requirements. By applying effective data masking techniques, NTIL ensures data privacy while supporting operational flexibility and innovation in a secure and compliant manner.

d) **Data resilience**: Data resilience refers to the organization’s ability to withstand and quickly recover from any disruptions that affect data availability, such as hardware failures, cyberattacks, power outages, or natural disasters. It encompasses backup systems, disaster recovery planning, redundancy, and high availability infrastructure.

Ensuring strong data resilience helps minimize operational downtime and business impact. Rapid recovery capabilities are essential to maintaining continuity and protecting critical operations.

e) **Antivirus protection**

To safeguard NTIL's IT environment, antivirus protection is mandatory across all digital endpoints. This includes desktops, laptops, servers, and other client systems.

Antivirus Deployment and Maintenance

- All PCs, servers, laptops, and client systems must have licensed antivirus software installed and actively running.
- Virus definition updates and scanning engines must be regularly updated to the latest versions.
- Antivirus scans must be scheduled to run at regular intervals to ensure early detection and mitigation of threats.
- Infected machines must be immediately disconnected from the network to prevent further spread until verified as virus-free.
- Periodic audits must be conducted across all user systems to confirm the use of current antivirus software and that no threats are active

Responses To a Virus Infection:

- Employees must immediately notify the IT Department if a virus infection is suspected or detected.

- The IT team will initiate containment and cleaning procedures, including virus removal and system repair.
- All virus incidents must be logged and documented in the Security Incident Management System.
- If cleanup is unsuccessful, the affected system's hard drive will be reformatted, and software will be reinstalled using clean, licensed versions.
- Infected systems posing a risk to the broader network will be isolated until they are fully cleared by IT technicians.

f) Hardware Failure

Hardware components such as servers, laptops, and storage devices are subject to wear and eventual failure. Such failures can compromise the integrity, availability, and confidentiality of critical business data and applications if not properly managed.

Mitigation Measures

- **Regular Backups**: All critical systems and data must be backed up at scheduled intervals and verified for recovery integrity.
- **Hardware Lifecycle Management**: IT must proactively monitor hardware health and maintain an inventory of assets nearing end-of-life for timely replacement.
- **Redundancy and Failover**: Redundant systems, clustering, or cloud-based failover solutions must be in place for critical infrastructure.
- **Monitoring and Alerts**: Hardware health should be continuously monitored through diagnostic tools and alerts configured for early warning signs of degradation or failure.

Contingency Planning

- The IT Department is responsible for establishing and maintaining hardware failure response protocols.
- Replacement hardware or standby systems should be readily available to ensure minimal disruption in the event of hardware failure.
- Lessons learned from failure incidents must be documented and reviewed during periodic IT risk assessments.

g) Network or Web Server Outages

Network and web server outages pose a substantial risk to business continuity, operational efficiency, and customer satisfaction. These disruptions may result from hardware malfunctions, software errors, misconfigurations, cyberattacks, or external factors such as ISP failures or natural disaster.

Mitigation Measures

- **Redundant Network Infrastructure**: Implement dual internet service providers (ISPs), backup network routes, and redundant server configurations to reduce single points of failure.

- **Uptime Monitoring**: Use real-time monitoring tools for early detection of downtime or latency issues across network and server infrastructure.
- **Automatic Failover Systems**: Deploy load balancers, clustering, or cloud-based redundancy for web servers and critical business applications.
- **Disaster Recovery Plans (DRP)**: Maintain and regularly test a DRP that outlines protocols for restoring network and server functionality within defined recovery time objectives (RTOs).
- **Change Management**: Ensure controlled and well-documented changes to network or web server configurations to avoid unplanned outages.

Response Protocol

- The IT Department must respond immediately to outages, isolate root causes, and restore services as quickly as possible.
- Outage incidents must be recorded in the Security or IT Incident Management System for tracking, post-mortem analysis, and continuous improvement.

7. **Advanced Data Security Measures**
   To fortify the organization's IT Security posture and respond to the evolving threat landscape, NTIL has implemented the following advanced data security measures:

- **Artificial Intelligence (AI):**
  AI technologies enhance the organization's data security framework by analysing vast volumes of data in real time. Through cognitive computing, a branch of AI, the system can simulate human decision-making processes, enabling swift and intelligent responses to security threats and incidents.
- **Multi-Level Security:**
  NTIL employs a multi-layered security architecture to protect critical data, applications, and proprietary processes across hybrid cloud environments. Employees are mandated to store data on local devices with parallel backups to secure cloud platforms to ensure redundancy and data resilience.
- **Quantum Security:**
  As part of its forward-looking security strategy, NTIL is exploring the integration of quantum encryption algorithms that offer enhanced protection against advanced cyber threats. This emerging technology is expected to redefine the standards of cryptographic security.
- **Defence-in-Depth Security Strategy:**
  The organization applies a layered defence model incorporating anti-malware, antivirus software, firewalls, email and web security filters, application allowlisting/denylisting, and real-time monitoring tools to ensure comprehensive asset protection.
- **Advanced Protection Technologies:**
  NTIL deploys cutting-edge tools such as Extended Detection and Response (XDR), Managed Detection and Response (MDR), User and Entity Behaviour Analytics (UEBA), and Zero-Trust Architecture to identify, prevent, and mitigate complex cyber threats proactively.
- **Regular Patching and Updates:**
  All systems, software applications, and IT infrastructure components are regularly updated with the latest security patches to eliminate known vulnerabilities and ensure optimal protection.

- **Frequent Data Backups:**
  Regular, secure backups of critical organizational data are performed and stored in both cloud and offline systems. This ensures business continuity and data restoration in the event of cyberattacks, system malfunctions, or other unforeseen incidents.

8. **DISCIPLINARY ACTION**
   NTIL enforces a zero-tolerance approach toward violations of its IT Security Policy. Any individual—whether an employee, contractor, consultant, or third-party service provider—found to be in breach of this policy will be subject to disciplinary action, depending on the nature and severity of the infraction.

a. **Warning or Reprimand:** In accordance with the *Industrial Employment (Standing Orders) Act, 1946*, and as outlined in the Model Standing Orders, a formal warning or reprimand may be issued for minor or first-time violations as a corrective measure.
b. **Suspension:** As per *Section 33 of the Industrial Disputes Act, 1947*, NTIL reserves the right to suspend an employee during an inquiry related to serious violations or misconduct involving data security or IT Security breaches.
c. **Termination of Employment:** Termination may be executed under *Section 25F of the Industrial Disputes Act, 1947* for workmen and employment contract provisions and organizational policies for managerial and non-workman employees.
d. **Monetary Penalty or Deduction from Salary:** Under *Section 7 of the Payment of Wages Act, 1936*, NTIL may deduct monetary penalties from wages in cases of willful negligence resulting in data loss or damages, subject to procedural fairness and documentation.
e. **Legal Proceedings for Data Theft or Cybercrime:** Violations involving unauthorized access, misuse, theft, or disclosure of sensitive information may result in legal action under relevant statutory frameworks, including:
   - Bharatiya Nyaya Sanhita (BNS), 2023:
     - ➢ Sections 316 & 317: Criminal breach of trust involving misuse of company data
     - ➢ Sections 151–153: Cyber offenses including unauthorized access, hacking, and digital data theft
   - Digital Personal Data Protection Act, 2023: Covers civil and criminal liabilities for unauthorized data processing or disclosure.
   - Information Technology Act, 2000
     - ➢ Section 43: Penalties for unauthorized access and data theft
     - ➢ Section 66: Punishment for hacking and data tampering
     - ➢ Section 72: Penalty for breach of confidentiality and privacy obligations

NTIL is committed to ensuring that all incidents are investigated fairly and that due process is followed in every case. Disciplinary actions will be documented and may involve consultation with legal and compliance teams, especially where statutory violations are suspected.

9. **REVIEW & REVISION**
   This policy will be reviewed periodically to ensure its effectiveness and compliance with evolving laws and best practices. Updates or revisions will be communicated to all employees.

****