CYBER SECURITY POLICY
Process Owner: IT Department
Intended Users: ABNT Group - All Users

Last Updated: 23 Feb 2023

Version 3.1

1. Purpose

The purpose of this Cyber Security Policy is to establish the principles and guidelines for safeguarding the confidentiality, integrity, and availability of ABNT Global Sdn Bhd's (ABNT) information assets and information technology (IT) systems. This policy outlines the approach to identifying, managing, and mitigating cyber risks to prevent unauthorized access, disclosure, modification, or destruction of ABNT's data and systems.

ABNT is committed to maintaining the highest standards of cyber security to protect the organization's critical business operations, intellectual property, and data integrity.

2. Scope

This policy applies to all employees, contractors, consultants, third-party vendors, and other external entities who have access to ABNT's information systems, networks, and data. It encompasses all devices, infrastructure, software applications, and cloud services used within the organization. The policy applies across all of ABNT's offices, data centers, and remote working environments.

3. Roles and Responsibilities

- **Board of Directors**: Ensure that cyber security is prioritized at the executive level, aligning resources and strategy with organizational objectives.

- **Senior Management**: Oversee the implementation of the cyber security framework, allocate necessary resources, and ensure compliance with the policy across all levels of the organization.

- **Cyber Security Officer (CSO)**: The CSO is responsible for managing and enforcing cyber security protocols. This includes risk assessment, monitoring, training, and response to security incidents. The CSO also serves as the liaison for all security-related matters within ABNT.

- **IT Department**: The IT department is tasked with maintaining and securing ABNT's IT infrastructure. This includes implementing firewalls, intrusion prevention systems, regular software updates, and patch management.

- **Employees and Contractors**: Every individual with access to ABNT's IT systems is responsible for adhering to the security policies, reporting any vulnerabilities or security incidents, and using IT resources responsibly.

4. Cyber Security Principles
ABNT Global is committed to protecting its information assets by adhering to the following fundamental principles:

- **Confidentiality**: Ensuring that sensitive and proprietary information is accessed only by authorized users.

- **Integrity**: Maintaining the accuracy, consistency, and reliability of data and systems, ensuring no unauthorized modification or tampering.

- **Availability**: Ensuring that information systems, networks, and data are accessible to authorized users as needed, with minimal downtime or disruption.

- **Accountability**: Implementing mechanisms to track access, usage, and changes to systems and data, ensuring transparency and accountability.

5. Cyber Risk Management
ABNT Global takes a proactive approach to managing cyber security risks, employing the following processes:

- **Risk Assessment**: Regular, comprehensive risk assessments will be conducted to identify potential vulnerabilities in our information systems. The findings will be used to assess the likelihood and impact of identified risks and to determine appropriate mitigation measures.

- **Risk Mitigation**: Once risks are identified, appropriate control measures will be put in place to minimize or eliminate potential threats. This includes technological measures, employee training, and changes to organizational practices.

- **Incident Response**: ABNT will maintain a robust incident response plan to ensure that all potential breaches or security incidents are handled efficiently. The CSO will be responsible for managing the response, minimizing damage, and reporting incidents to relevant authorities as required.

6. Access Control and Authentication
ABNT enforces strict access control policies to protect critical systems and sensitive data:

- **User Access Management**: Each employee, contractor, and third-party user is assigned a unique user ID and is required to authenticate using secure, multifactor authentication (MFA) mechanisms.

- **Least Privilege Principle**: Access to data and systems will be granted based on the principle of least privilege. Users will only be provided with the minimum level of access required to perform their duties.

- **Privileged Access**: Administrative accounts and other privileged access accounts will be strictly controlled and monitored. These accounts will be reviewed regularly to ensure compliance with security standards.

7. Data Protection and Encryption
Data security is a critical component of ABNT's cyber security framework:

- **Data Classification**: All data within ABNT will be classified according to sensitivity and confidentiality levels. Sensitive data, including personal data and intellectual property, will receive heightened protection.

- **Data Encryption**: ABNT will use strong encryption protocols for data both in transit and at rest, ensuring that unauthorized individuals cannot access or compromise the data. This includes encryption of communications over the network and securing stored data.

- **Data Retention and Disposal**: ABNT will retain data only for the period necessary for business and legal purposes. Data that is no longer needed will be securely disposed of in accordance with industry standards to prevent unauthorized retrieval.

8. Network Security
To protect ABNT's internal network and connected systems, we implement the following network security measures:

- **Firewall Protection**: Firewalls will be configured to block unauthorized access while allowing legitimate business traffic. These firewalls will be regularly updated and maintained.

- **Intrusion Detection and Prevention Systems (IDPS)**: ABNT will deploy systems to monitor network traffic for unusual or suspicious activity. Alerts will be generated for potential security incidents, and appropriate response actions will be initiated.

- **Virtual Private Networks (VPNs)**: Employees accessing ABNT systems remotely will use secure VPNs to encrypt their internet traffic and ensure the privacy of their communications.

9. Security Awareness and Training
ABNT is committed to maintaining a well-informed workforce with the skills to identify and respond to cyber security threats:

- **Employee Training**: All employees will undergo regular security awareness training. The training will include topics such as identifying phishing attacks, creating strong passwords, handling sensitive information, and reporting security incidents.

- **Ongoing Education**: Employees will be kept informed about the latest cyber threats and security best practices through regular updates and refresher courses.

10. Third-Party and Vendor Management
ABNT recognizes that third-party vendors and contractors may pose potential security risks:

- **Third-Party Risk Assessment**: All third-party vendors and partners who have access to ABNT systems or data will undergo a thorough security assessment before entering into any business relationship.

- **Contractual Security Obligations**: All contracts with third-party vendors will include clauses that specify cyber security requirements, including data protection measures and reporting obligations.

- **Third-Party Audits**: ABNT reserves the right to audit the cyber security practices of its third-party vendors to ensure they meet our security standards.

11. Compliance and Legal Requirements
ABNT is committed to complying with all relevant laws, regulations, and standards governing cyber security and data protection, including:

- **Personal Data Protection Act (PDPA)**: ABNT complies with Malaysia's PDPA and any other relevant data protection regulations.

- **ISO/IEC 27001**: ABNT will aim to comply with ISO/IEC 27001 standards for information security management systems.

- **Other Legal Requirements**: ABNT will adhere to all applicable national and international legal frameworks related to cyber security and data privacy.

12. Incident Reporting and Management

- **Incident Reporting**: Any employee or stakeholder who suspects a security breach must immediately report the incident to the Cyber Security Officer (CSO). A dedicated channel will be provided for secure reporting of potential security issues.

- **Incident Investigation and Response**: ABNT will conduct thorough investigations of any reported incidents, and appropriate remedial actions will be taken to mitigate damage and prevent recurrence.

13. Monitoring and Auditing

- **Continuous Monitoring**: ABNT will continuously monitor network traffic, system logs, and user activity to detect and respond to potential threats in real-time.

- **Regular Audits**: Regular internal and external security audits will be conducted to assess the effectiveness of the security measures and ensure compliance with this policy.

14. Policy Review and Updates

ABNT will review this Cyber Security Policy at least annually, or whenever significant changes in technology or regulatory requirements occur. Updates will be communicated to all employees, and any changes will be incorporated into training programs.

Chief Executive Officer
ABNT Global Sdn Bhd