Data Privacy and Cybersecurity Policy

1. Policy Objective

The objective of this Data Privacy and Cybersecurity Policy is to ensure that **Miten** protects sensitive information, maintains data integrity, and secures its digital infrastructure from unauthorized access, data breaches, and cyber threats. This policy aims to support regulatory compliance, promote responsible data handling, and build a resilient cybersecurity culture across all company operations.

2. Scope

This policy applies to all employees, contractors, vendors, and third parties who access, process, or manage data in **Miten**'s systems. It covers all digital assets, including internal systems, client data, project documentation, and any technology infrastructure used across sectors like energy, renewable energy, hydropower, transmission infrastructure, agribusiness, food processing, warehousing, and cold storage.

3. Core Principles

A. Data Privacy and Protection

1. **Data Confidentiality and Integrity**
   - Ensure the confidentiality, integrity, and availability of all data, particularly sensitive information related to employees, clients, and partners.
2. **Compliance with Data Privacy Laws**
   - Adhere to all applicable data privacy laws, such as the General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA), and other relevant regulations governing data protection.

B. Cybersecurity and Threat Prevention

1. **Proactive Threat Management**
   - Implement proactive cybersecurity measures, including risk assessments, vulnerability testing, and incident response planning, to defend against potential cyber threats.
2. **Network and System Security**
   - Maintain robust security protocols, such as firewalls, encryption, and access controls, to protect digital assets and prevent unauthorized access.

C. Transparency and Accountability

1. **Data Usage Transparency**
   - Ensure transparent communication regarding data collection, usage, and storage practices, providing individuals with control over their personal information where applicable.

2. **Clear Accountability Structure**
    - Assign specific roles and responsibilities for data protection and cybersecurity within the organization to promote accountability and compliance.

4. Data Privacy Standards

A. Data Collection and Processing

1. **Data Minimization**
    - Collect only the data necessary for specific business purposes, ensuring data is relevant, accurate, and limited to what is needed for operational functions.
2. **Lawful Basis for Data Processing**
    - Obtain consent where required and ensure a lawful basis for processing personal data in alignment with applicable regulations.

B. Data Storage and Retention

1. **Data Retention Policies**
    - Establish data retention schedules to ensure that personal and sensitive data is stored only for as long as necessary and securely deleted when no longer required.
2. **Secure Storage Solutions**
    - Utilize secure storage solutions, including encryption and access controls, for sensitive data and regularly review storage practices for compliance with regulatory standards.

C. Access Control and Data Sharing

1. **Access Control Mechanisms**
    - Implement role-based access controls (RBAC) to ensure that only authorized personnel have access to specific data sets, with regular reviews to adjust permissions as needed.
2. **Third-party Data Sharing Compliance**
    - Establish data-sharing agreements with third-party vendors and partners, ensuring they comply with data protection standards and restrict access to necessary information only.

5. Cybersecurity Measures

A. Network Security

1. **Firewalls and Intrusion Detection**
    - Deploy firewalls and intrusion detection systems (IDS) to monitor network activity and detect suspicious behavior that may indicate a security threat.
2. **Secure Remote Access**

- Secure remote access with VPNs and multi-factor authentication (MFA) for employees and contractors who access company systems from remote locations.

B. Endpoint Protection

1. **Anti-virus and Anti-malware Solutions**
    - Install and regularly update anti-virus and anti-malware software on all endpoints to protect devices from malicious software.
2. **Mobile Device Management (MDM)**
    - Enforce MDM policies to secure mobile devices, ensuring that devices accessing company data meet security requirements and can be remotely managed or wiped if lost or stolen.

C. Data Encryption

1. **Encryption Standards**
    - Use industry-standard encryption protocols (e.g., AES-256) to protect data in transit and at rest, ensuring sensitive data remains secure against unauthorized access.
2. **End-to-End Encryption for Communications**
    - Implement end-to-end encryption for all sensitive communications, including emails and data exchanges, to prevent interception.

D. Regular Security Assessments

1. **Vulnerability Scanning**
    - Conduct regular vulnerability scans to identify and address potential security weaknesses in systems, networks, and applications.
2. **Penetration Testing**
    - Perform periodic penetration testing to simulate cyber attacks and assess the resilience of the company's security defenses.

6. Incident Response and Management

A. Incident Response Plan

1. **Incident Response Framework**
    - Develop an incident response plan that includes procedures for detecting, reporting, and responding to cybersecurity incidents.
2. **Incident Response Team (IRT)**
    - Establish an Incident Response Team responsible for managing and mitigating cybersecurity incidents, including containment, recovery, and communication with stakeholders.

B. Reporting and Documentation

1. **Incident Reporting Protocols**
    - Implement clear reporting protocols to ensure prompt reporting and escalation of incidents within the company, with procedures for notifying affected individuals and regulatory authorities if necessary.
2. **Documentation and Post-Incident Review**
    - Document all incidents and conduct post-incident reviews to analyze root causes, improve response strategies, and implement lessons learned.

7. Data Breach Prevention and Management

A. Breach Prevention Strategies

1. **Regular Data Audits**
    - Perform data audits to ensure data handling practices comply with privacy policies, identifying and addressing potential vulnerabilities.
2. **Employee Training on Data Protection**
    - Train employees on data privacy best practices, such as identifying phishing attempts, securing devices, and adhering to company policies on data handling.

B. Data Breach Response

1. **Immediate Containment Measures**
    - Take immediate action to contain data breaches, preventing further unauthorized access and securing affected systems.
2. **Breach Notification Protocols**
    - Follow legal requirements for notifying regulatory authorities and affected individuals in case of a data breach, as required by data privacy laws (e.g., GDPR, CCPA).

8. Training and Awareness

A. Cybersecurity Training Programs

1. **Mandatory Training for Employees and Contractors**
    - Provide mandatory cybersecurity training for all employees and contractors, covering topics such as data protection, threat identification, and safe online practices.
2. **Role-specific Training**
    - Offer additional training for employees handling sensitive information or working with IT infrastructure, focusing on role-specific security requirements and best practices.

B. Security Awareness Campaigns

1. **Regular Awareness Initiatives**

   - Run security awareness campaigns to keep employees informed about emerging cybersecurity threats and safe data handling practices.
2. **Phishing Simulations and Drills**
   - Conduct regular phishing simulations and cybersecurity drills to assess employee preparedness and reinforce training.

9. Compliance and Governance

A. Compliance with Data Protection Regulations

1. **Regulatory Compliance Tracking**
   - Continuously monitor changes in data protection and cybersecurity regulations, ensuring compliance with applicable laws across all regions where the company operates.
2. **Data Protection Officer (DPO)**
   - Appoint a Data Protection Officer responsible for overseeing data privacy compliance, handling data subject requests, and serving as the point of contact with regulatory bodies.

B. Internal Audits and Third-Party Assessments

1. **Regular Internal Audits**
   - Conduct internal audits to assess compliance with data privacy and cybersecurity policies, addressing any identified gaps promptly.
2. **Third-Party Security Assessments**
   - Engage third-party security experts to perform independent assessments of the company’s cybersecurity infrastructure and policies.

C. Accountability and Oversight

1. **Cybersecurity Governance Committee**
   - Establish a governance committee responsible for overseeing cybersecurity strategy, policy compliance, and continuous improvement.
2. **Clear Reporting Structure**
   - Define a reporting structure for data privacy and cybersecurity matters, ensuring senior management is informed of critical issues and emerging risks.

10. Policy Review and Continuous Improvement

1. **Annual Policy Review**
   - Review this Data Privacy and Cybersecurity Policy annually to ensure its relevance and effectiveness in light of evolving security threats, regulatory updates, and technological advancements.
2. **Continuous Improvement**

- Integrate lessons learned from security incidents, audits, and industry best practices to enhance cybersecurity measures and strengthen data privacy controls.

Contact Information

For inquiries about this Data Privacy and Cybersecurity Policy or to report a security concern, please contact:

- **Data Privacy and Cybersecurity Department**
- **Email:** info@mitenenerji.com

“The policy reinforces **Miten's** commitment to data privacy, information security, and proactive threat management, ensuring that our operations remain resilient and secure against emerging cyber risks.”

Miten Energy

Updated: 2017