EquipProtek Energy Cybersecurity Handbook

Table of Contents

1. Introduction

- Purpose of the Handbook
- Scope
- Importance of Cybersecurity

2. Cybersecurity Governance

- Roles and Responsibilities
- Cybersecurity Policy Overview
- Compliance with Legal and Regulatory Requirements

3. Information Security Policies

- Data Classification and Handling
- Access Control Policies
- Password Management
- Network Security
- Incident Response Policy

4. Employee Responsibilities

- Acceptable Use Policy
- Email and Communication Security

- Social Engineering Awareness
- Remote Work and Mobile Device Security
- Reporting Security Incidents

5. Technical Security Measures

- Firewall and Network Security
- Antivirus and Anti-malware Protection
- Encryption Standards
- Backup and Recovery Procedures
- System and Software Updates

6. Data Protection

- Personal Data Protection
- Third-Party Vendor Management
- Data Retention and Disposal
- Physical Security of IT Assets

7. Cybersecurity Training and Awareness

- Mandatory Training Programs
- Phishing Simulations
- Regular Security Updates and Communication

8. Incident Management

- Incident Detection and Reporting
- Incident Response Procedures
- Post-Incident Review and Documentation

9. Monitoring and Auditing

- Regular Security Audits
- Log Management and Monitoring
- Compliance Monitoring

10. Continuous Improvement

- Regular Policy Review and Updates
- Feedback and Improvement Mechanisms
- Staying Informed on Emerging Threats

11. Conclusion

- Commitment to Cybersecurity
- Contact Information for Security Concerns

1. Introduction

Purpose of the Handbook

The purpose of this handbook is to provide guidance and establish clear cybersecurity protocols to protect EquipProtek Energy's digital assets, confidential information, and IT infrastructure. It serves as a resource for all employees, contractors, and partners to understand their role in safeguarding the company against cyber threats.

Scope

This handbook applies to all employees, contractors, and third-party vendors who have access to EquipProtek Energy’s IT systems, data, and facilities. It covers all aspects of cybersecurity, from daily operational practices to incident response procedures.

Importance of Cybersecurity

As a company operating in the Oil, Gas, and Energy industries, EquipProtek Energy is a potential target for cyberattacks that could compromise sensitive data, disrupt

operations, or cause financial loss. Cybersecurity is crucial to maintaining the integrity, confidentiality, and availability of the company's information and systems.

2. Cybersecurity Governance

Roles and Responsibilities

- Executive Leadership: Oversee and support cybersecurity initiatives, ensuring alignment with business goals.

- IT Security Team: Implement and maintain cybersecurity measures, monitor threats, and respond to incidents.

- Employees: Adhere to cybersecurity policies, report suspicious activities, and participate in training.

- Third-Party Vendors: Comply with EquipProtek Energy’s cybersecurity requirements when handling company data or accessing systems.

Cybersecurity Policy Overview

EquipProtek Energy’s cybersecurity policies are designed to mitigate risks, protect assets, and ensure compliance with industry regulations. These policies are reviewed regularly and updated to address emerging threats.

Compliance with Legal and Regulatory Requirements

The company is committed to complying with all applicable laws, regulations, and standards related to cybersecurity, including those specific to the Oil, Gas, and Energy sectors.

3. Information Security Policies

Data Classification and Handling

- Data Classification: Information is categorized based on its sensitivity (e.g., Public, Internal, Confidential).

- Handling: Sensitive data must be encrypted and accessed only by authorized personnel.

Access Control Policies

- User Access: Access to systems and data is granted based on job roles and responsibilities.

- Multi-Factor Authentication (MFA): Required for accessing critical systems and sensitive information.

Password Management

- Password Requirements: Strong, unique passwords must be used for all accounts.

- Password Expiration: Passwords must be changed regularly, with a recommended expiration period of 90 days.

Network Security

- Firewalls: Protect internal networks from external threats.

- Virtual Private Network (VPN): Used for secure remote access to the company's network.

Incident Response Policy

- Incident Reporting: All security incidents must be reported immediately to the IT Security Team.

- Response Plan: The company has a defined process for identifying, containing, and resolving cybersecurity incidents.

4. Employee Responsibilities

Acceptable Use Policy

- IT Resources: Employees must use company IT resources for business purposes only and in accordance with company policies.

- Prohibited Activities: Unauthorized access, data manipulation, and sharing of sensitive information are prohibited.

Email and Communication Security

- Phishing Awareness: Employees must be vigilant against phishing attempts and report suspicious emails.

- Secure Communication: Sensitive information must be shared using secure methods, such as encrypted emails.

Social Engineering Awareness

Employees must be aware of social engineering tactics used by attackers to manipulate individuals into divulging confidential information or granting unauthorized access.

Remote Work and Mobile Device Security

- Remote Access: Employees must use company-approved methods to access the network remotely, such as VPNs.

- Mobile Device Management (MDM): Company data on mobile devices must be secured through MDM solutions.

Reporting Security Incidents

Employees are required to report any suspicious activities, potential security breaches, or vulnerabilities to the IT Security Team immediately.

5. Technical Security Measures

Firewall and Network Security

Firewalls are configured to block unauthorized access while allowing legitimate traffic. Regular updates and monitoring are conducted to ensure the network's security.

Antivirus and Anti-malware Protection

All company devices must have up-to-date antivirus and anti-malware software installed to protect against malicious software.

Encryption Standards

Sensitive data, both in transit and at rest, must be encrypted using industry-standard encryption protocols.

Backup and Recovery Procedures

Regular backups of critical data are performed and stored securely to ensure data can be recovered in case of a cyber incident or data loss.

System and Software Updates

All systems and software must be regularly updated to protect against vulnerabilities. Automatic updates should be enabled where possible.

6. Data Protection

Personal Data Protection

Personal data of employees, customers, and partners must be handled in accordance with data protection laws and company policies, ensuring privacy and security.

Third-Party Vendor Management

Vendors with access to company data or systems must adhere to EquipProtek Energy's cybersecurity standards. Regular assessments of vendor security practices are conducted.

Data Retention and Disposal

Data retention policies ensure that information is stored only as long as necessary. Secure methods must be used to dispose of data that is no longer needed.

Physical Security of IT Assets

Physical access to IT assets is restricted to authorized personnel. Devices must be secured when not in use, and portable devices must be stored securely.

7. Cybersecurity Training and Awareness

Mandatory Training Programs

All employees are required to complete cybersecurity training upon hiring and participate in regular refresher courses.

Phishing Simulations

The company conducts regular phishing simulations to test employee awareness and improve response to potential threats.

Regular Security Updates and Communication

Employees are kept informed about the latest security threats, policy changes, and best practices through regular communications from the IT Security Team.

8. Incident Management

Incident Detection and Reporting

Systems are in place to detect potential security incidents, and employees are trained to recognize and report suspicious activities immediately.

Incident Response Procedures

Upon detection of an incident, the IT Security Team will follow a structured response plan, including containment, eradication, recovery, and communication with stakeholders.

Post-Incident Review and Documentation

After resolving an incident, a thorough review is conducted to identify lessons learned and update policies and procedures accordingly.

9. Monitoring and Auditing

Regular Security Audits

The company conducts regular security audits to assess the effectiveness of its cybersecurity measures and ensure compliance with policies.

Log Management and Monitoring

System logs are monitored and reviewed to detect unauthorized access or suspicious activities, and logs are securely stored for future reference.

Compliance Monitoring

Regular checks are conducted to ensure that the company is in compliance with all relevant cybersecurity regulations and industry standards.

10. Continuous Improvement

Regular Policy Review and Updates

Cybersecurity policies are reviewed at least annually or as needed to address changes in the threat landscape, technology, or business operations.

Feedback and Improvement Mechanisms

Employees are encouraged to provide feedback on cybersecurity practices, and continuous improvement is sought through regular evaluations and updates.

Staying Informed on Emerging Threats

The IT Security Team monitors emerging cybersecurity threats and adapts policies and practices to protect against new risks.

11. Conclusion

EquipProtek Energy is committed to maintaining a secure and resilient IT environment. Cybersecurity is a shared responsibility, and the cooperation of all employees, contractors, and partners is essential in safeguarding our digital assets and ensuring the continued success of our operations.

For any cybersecurity concerns or inquiries, please contact the IT Security Team at Contact Information: ithelp@equipprotek.com