INFORMATION TECHNOLOGY (IT) SECURITY POLICY

Introduction

ADVANCED ENGINEERING GROUP (the "Company"), based in the United Kingdom, recognizes the critical importance of information security in safeguarding our assets, ensuring business continuity, and maintaining the trust of our clients, partners, and stakeholders. This policy outlines the principles, guidelines, and responsibilities for protecting the Company's information assets and IT infrastructure from unauthorized access, disclosure, alteration, or destruction.

Scope

This IT Security Policy applies to all employees, contractors, third-party vendors, and affiliates who have access to the Company's information systems, networks, and data. It covers all devices, systems, and data owned, operated, or managed by ADVANCED ENGINEERING GROUP.

Company Structure

Headquartered in SILSDEN, UK, ADVANCED ENGINEERING GROUP operates internationally through various legal entities, including:

- **ADVANCED ACTUATORS LIMITED**
- **ADVANCED COMPONENTS LIMITED**
- **ADVANCED DRIVES**

Policy Statement

- **Data Protection:** All employees are responsible for protecting the confidentiality, integrity, and availability of the Company's data. Access to sensitive or confidential information should be restricted to authorized personnel only, and data should be handled in accordance with applicable data protection laws and regulations, including the General Data Protection Regulation (GDPR).

- **Access Control:** Access to IT resources and systems should be granted based on the principle of least privilege. User access rights should be reviewed regularly and revoked promptly when no longer necessary. Strong authentication mechanisms, such as passwords, multi-factor authentication, and access controls, should be implemented to prevent unauthorized access.

- **Network Security:** The Company's network infrastructure should be protected against unauthorized access, interception, or tampering. Firewalls, intrusion detection/prevention systems, and encryption should be used to secure network communications. Wireless networks should be encrypted and segregated from the internal network.

- **Endpoint Security:** All devices (e.g., computers, laptops, mobile devices) connected to the Company's network should be equipped with up-to-date security software, including antivirus/antimalware programs, endpoint detection and response (EDR) tools, and host-based firewalls. Employees should follow best practices for securing their devices, including regular software updates and patches.

- **Information Security Awareness:** All employees should receive regular training and awareness programs on IT security best practices, including phishing awareness, password hygiene, social engineering attacks, and incident response procedures. Reporting mechanisms should be in place to report suspected security incidents promptly.

ADVANCED ENGINEERING GROUP
Unit 4, Ryefield Way, Silsden,
West Yorkshire, BD20 0EF, England
+44 (0) 1535 655 151
sales@ae.group

- **Incident Response:** The Company maintains an incident response plan to address security incidents, breaches, or suspected compromises promptly. Employees should report any security incidents or suspicious activities to the IT security team or designated incident response personnel for investigation and remediation.

Responsibilities

- **Management:** The management team is responsible for providing leadership, resources, and support for the implementation and enforcement of this IT Security Policy.
- **IT Security Team:** The IT security team is responsible for developing, implementing, and maintaining IT security measures, conducting risk assessments, monitoring security controls, and responding to security incidents.
- **Employees:** All employees are responsible for complying with this policy, following security best practices, and reporting any security concerns or incidents promptly.

Compliance and Enforcement

Non-compliance with this IT Security Policy may result in disciplinary action, including warnings, suspension, termination of employment, or legal action, depending on the severity of the violation. All employees, contractors, and third-party vendors are required to adhere to this policy and cooperate with IT security personnel during security audits, assessments, or investigations.

Training and Awareness

Training Notes are attached to this Policy and should be read by all employees; anyone requiring any further guidance or external training should notify your line manager or a Director of the company

Policy Review and Updates

This IT Security Policy will be reviewed annually and updated as necessary to address emerging threats, changes in technology, regulatory requirements, or business needs. Employees will be notified of any changes to the policy, and updated training and awareness programs will be provided as needed.

This policy has been endorsed and approved by:



Andrew Peace
Managing Director

Date: 1st June 2026

ADVANCED ENGINEERING GROUP
Unit 4, Ryefield Way, Silsden,
West Yorkshire, BD20 0EF, England
+44 (0) 1535 655 151
sales@ae.group

TRAINING NOTES

Introduction

This appendix provides detailed Information Technology (IT) security policies for Advanced Engineering Group, a UK based engineering business engaged in both domestic and international operations, including exports. These policies aim to protect our digital assets, ensure the integrity and confidentiality of sensitive information, comply with relevant legal and regulatory requirements, and support business continuity.

IT SECURITY POLICY OBJECTIVES

- **Protect Digital Assets**: Safeguard all digital assets, including intellectual property, customer data, and proprietary information, from unauthorized access, theft, or damage.
- **Ensure Compliance**: Adhere to relevant legal and regulatory requirements, including data protection laws (e.g., GDPR), export controls, and industry standards.
- **Maintain Business Continuity**: Implement measures to ensure the continuity of IT services and minimize disruptions due to security incidents.
- **Promote Cybersecurity Awareness**: Foster a culture of cybersecurity awareness among employees and stakeholders to mitigate risks.

IT SECURITY MEASURES

Access Control

- **User Authentication**: Implement multi-factor authentication (MFA) for all users accessing the company's IT systems to enhance security.
- **Role-Based Access**: Assign access rights based on the principle of least privilege, ensuring that employees only have access to the information necessary for their roles.
- **Password Management**: Enforce strong password policies, including regular password changes, complexity requirements, and secure storage of passwords.
- **Access Reviews**: Conduct regular reviews of user access rights to ensure compliance with access control policies and remove unnecessary privileges.

Data Protection

- **Encryption**: Use encryption technologies to protect sensitive data both at rest and in transit, ensuring that only authorized parties can access the data.
- **Data Backup**: Regularly back up critical data and store backups in secure, offsite locations to ensure data recovery in case of a breach or disaster.
- **Data Classification**: Implement a data classification scheme to identify and handle sensitive information appropriately, ensuring that it receives the necessary level of protection.
- **Data Loss Prevention (DLP)**: Deploy DLP solutions to detect and prevent potential data breaches by monitoring and controlling data flows.

Network Security

- **Firewall and Intrusion Detection Systems (IDS)**: Deploy firewalls and IDS to monitor and protect the company's network from unauthorized access and cyber threats.
- **Virtual Private Network (VPN)**: Require the use of VPNs for remote access to the company's network to ensure secure communication channels.
- **Network Segmentation**: Segment networks to limit the spread of potential breaches and protect critical systems from less secure areas of the network.
- **Secure Wi-Fi**: Ensure that all wireless networks are secured using strong encryption methods, such as WPA3, and implement guest network policies.

ADVANCED ENGINEERING GROUP
Unit 4, Ryefield Way, Silsden,
West Yorkshire, BD20 0EF, England
+44 (0) 1535 655 151
sales@ae.group

Endpoint Security

- **Antivirus and Anti-Malware**: Install and regularly update antivirus and anti-malware software on all company devices to protect against malicious software.
- **Device Management**: Implement endpoint management solutions to monitor, manage, and secure all endpoints, including laptops, mobile devices, and IoT devices.
- **Patch Management**: Ensure all software and systems are regularly updated with the latest security patches and updates to protect against known vulnerabilities.

Incident Response

- **Incident Response Plan**: Develop and maintain an incident response plan to quickly and effectively address IT security incidents, minimizing damage and recovery time.
- **Incident Reporting**: Establish clear procedures for reporting and escalating security incidents, including contact information for the IT security team.
- **Post-Incident Review**: Conduct thorough reviews and analyses of security incidents to identify root causes and implement preventive measures.
- **Incident Response Team (IRT)**: Form an IRT with defined roles and responsibilities to coordinate and manage responses to security incidents.

COMPLIANCE AND MONITORING

- **Legal and Regulatory Compliance**: Ensure compliance with relevant legal and regulatory requirements, including the General Data Protection Regulation (GDPR) and export control regulations.
- **Audits and Assessments**: Conduct regular security audits and risk assessments to evaluate the effectiveness of IT security measures and identify areas for improvement.
- **Continuous Monitoring**: Implement continuous monitoring of IT systems to detect and respond to security threats in real-time.
- **Compliance Reporting**: Regularly report on compliance status and security metrics to senior management and relevant regulatory bodies.

BUSINESS CONTINUITY AND DISASTER RECOVERY

- **Business Continuity Plan (BCP)**: Develop and maintain a BCP to ensure critical business functions can continue during and after a disaster.
- **Disaster Recovery Plan (DRP)**: Create a DRP to outline procedures for recovering IT systems and data following a disruptive event.
- **Testing and Drills**: Conduct regular testing and drills of BCP and DRP to ensure preparedness and identify areas for improvement.
- **Redundancy and Failover**: Implement redundancy and failover mechanisms for critical systems to minimize downtime in case of hardware or software failures.

VENDOR AND THIRD-PARTY MANAGEMENT

- **Contracts and SLAs**: Include security requirements and performance metrics in contracts and Service Level Agreements (SLAs) with vendors.
- **Third-Party Access Control**: Monitor and control third-party access to company systems and data, ensuring they follow the same security protocols as internal users.

Conclusion

By adhering to these IT security policies, Advanced Engineering Group aims to protect its digital assets, ensure compliance with legal and regulatory requirements, and maintain the trust of its customers and stakeholders. Continuous improvement and vigilance are key to maintaining a robust IT security posture in an ever-evolving threat landscape. This appendix serves as a crucial part of our overall security strategy, providing detailed guidance to safeguard our information technology infrastructure.

ADVANCED ENGINEERING GROUP
Unit 4, Ryefield Way, Silsden,
West Yorkshire, BD20 0EF, England
+44 (0) 1535 655 151
sales@ae.group