



Atlas Electrical & Security Ltd

Information Security Policy & Security Standards

Version 1.0 – Initial Issue

Policy Owner	Stephen Norton
Compliance Manager	James Whitcher
Director of IT	Christopher Wright
Date Approved	July 2026 (Version 1) Initial Issue
Review Date	July 2027

Atlas Electrical & Security Ltd

Registered Address Unit 2, Victoria Mill Business
Park, Wharf Road, Doncaster, South Yorkshire,
DN1 2ST

VAT Registration Number GB 175 3645 88

Registered in England & Wales No. 11548394

01302 400 218

www.atlassecurity.services

Atlas Electrical & Security Ltd – Information Security Policy & Security Standards

1. Purpose

This policy defines the information security requirements and minimum-security standards applicable to Atlas Electrical & Security Ltd. The objective is to protect customer information, company information, security systems, credentials, infrastructure and business operations.

2. Scope

Applies to all employees, directors, contractors, consultants, temporary workers, third-party suppliers and any person with access to Atlas information assets or customer systems.

3. Security Principles

Atlas shall maintain the confidentiality, integrity and availability of information. Security controls shall be proportionate to risk and reviewed regularly.

4. Roles and Responsibilities

Managing Director: overall accountability. Director of IT: security governance, access control, cyber security, incident response and technical standards. Compliance Manager: audits, compliance and awareness. Employees: compliance and incident reporting.

5. Access Control Standard

Unique user accounts are mandatory. Shared accounts are prohibited unless technically unavoidable and formally approved. Access shall follow least privilege and be reviewed periodically. Accounts shall be removed promptly when no longer required.

New user accounts shall only be created by the Director of IT. User permissions shall be reviewed when roles change. User accounts shall be disabled promptly when employment or engagement ends. Access rights shall be reviewed periodically and recorded by the Director of IT.

5a. Engineer Access

Engineers shall only be granted access to customer systems necessary for their role.

Access to customer systems shall be removed when no longer required.

Administrative access shall be controlled and approved by the Director of IT.

Atlas Electrical & Security Ltd

Registered Address Unit 2, Victoria Mill Business Park, Wharf Road, Doncaster, South Yorkshire, DN1 2ST

VAT Registration Number GB 175 3645 88

Registered in England & Wales No. 11548394

01302 400 218

www.atlassecurity.services

6. Password & Authentication Standard

NordPass is the Company's approved password management platform and shall be used for the storage and management of business credentials. Passwords must never be shared through email, messaging platforms or paper records. MFA is mandatory for Microsoft 365 and all supported critical systems. Users must not reuse business passwords across services.

Password Requirements

Passwords shall:

- Be at least 12 characters in length, containing at least one capital letter, one lowercase letter, one number and one special character.
- Be unique to each system.
- Not contain easily guessed information (eg. Name or username)
- Never be shared with unauthorised persons.

7. Customer Credential Management

Customer credentials, alarm codes, CCTV passwords, VPN credentials and administrator accounts are confidential. Access shall be authorised by the Director of IT. Credentials must be stored only within approved secure systems. Customer credentials must never be stored in personal password managers or unsecured spreadsheets.

8. Microsoft 365 Security Standard

Microsoft 365 Business Premium shall be the approved collaboration platform. OneDrive and SharePoint are the approved cloud storage locations. Security features, conditional access controls and MFA shall remain enabled.

9. Endpoint Security Standard

Company laptops and managed devices shall utilise Sophos Endpoint Protection. Security updates shall be installed promptly. Users must not disable antivirus, endpoint protection or security monitoring controls. Company laptops storing business information shall utilise Microsoft BitLocker full disk encryption where technically supported.

10. Remote Access & VPN Standard

Approved remote access solutions include TeamViewer and authorised VPN technologies. IPSec VPN tunnels shall utilise AES-256 encryption or equivalent approved standards. Remote access shall only be provided where there is a legitimate business requirement.

11. Mobile Device Security

Devices shall be protected by screen locks, passwords or PINs. Lost or stolen devices must be reported immediately. Sensitive information must not be left visible or unattended.

12. Email & Phishing Protection

Users must remain vigilant against phishing, business email compromise and social engineering. Suspicious emails, attachments and links must be reported immediately to the Director of IT.

Atlas Electrical & Security Ltd

Registered Address Unit 2, Victoria Mill Business Park, Wharf Road, Doncaster, South Yorkshire, DN1 2ST

VAT Registration Number GB 175 3645 88

Registered in England & Wales No. 11548394

01302 400 218

www.atlassecurity.services

13. Data Classification & Storage

Information shall be treated according to sensitivity. Customer data, credentials and security system information shall be treated as confidential. Approved storage locations include Microsoft OneDrive, SharePoint and authorised business systems. Personal data shall be retained and disposed of in accordance with the Company's GDPR Policy and applicable legal requirements.

14. Backup & Recovery Standard

Atlas utilises Veeam backup solutions. Backup restore testing shall be undertaken at least annually or following significant infrastructure changes. Backup failures shall be investigated and corrected promptly.

15. Physical Security

Company premises, vehicles, laptops, documents and storage media shall be protected against unauthorised access, theft and loss. Customer information must not be left unattended in vehicles.

16. Bring Your Own Device (BYOD)

Personal devices used for business activities require approval from the Director of IT and must meet security requirements including screen locking and software updates.

17. Supplier & Third-Party Security

Technology providers and suppliers may be subject to due diligence. Access to company systems shall be restricted to authorised and approved third parties.

18. Security Incident Management

Security incidents include phishing attacks, malware, ransomware, credential compromise, unauthorised access, data breaches and lost devices. Incidents must be reported immediately. The Director of IT shall coordinate response and remediation.

19. Logging, Monitoring & Audit

Atlas may monitor systems, access logs, security alerts and user activity where appropriate to protect company and customer information. Audits may be undertaken to verify compliance.

20. Training & Awareness

Security awareness training shall be provided during induction and periodically thereafter. Personnel shall remain aware of current cyber threats and security responsibilities.

21. Disciplinary Action

Failure to comply with this policy may result in disciplinary action, removal of access privileges, contractual action or legal action where appropriate.

22. Related Documents

GDPR Policy, Vehicle & Driving for Work Policy, Mobile Phones Policy, CCTV Policy, Anti-Bribery Policy, Whistleblowing Policy and relevant IT procedures.

Atlas Electrical & Security Ltd

Registered Address Unit 2, Victoria Mill Business Park, Wharf Road, Doncaster, South Yorkshire, DN1 2ST

VAT Registration Number GB 175 3645 88

Registered in England & Wales No. 11548394

01302 400 218

www.atlassecurity.services

23. Review

This policy shall be reviewed annually or following significant business, legal or technological changes.

Appendix A - Minimum Security Standards

- MFA enabled on supported systems.
- Company-approved password manager (NordPass).
- Sophos Endpoint Protection on managed devices.
- Approved cloud storage limited to OneDrive and SharePoint.
- Veeam backups maintained and monitored.
- Customer credentials controlled by the Director of IT.
- Immediate reporting of security incidents.
- AES-256 encrypted IPSec VPNs where deployed.

Signature Christopher Wright

Position: Director of IT

Signature: Stephen Norton

Position: Managing Director

Atlas Electrical & Security Ltd

Registered Address Unit 2, Victoria Mill Business Park, Wharf Road, Doncaster, South Yorkshire, DN1 2ST

VAT Registration Number GB 175 3645 88

Registered in England & Wales No. 11548394

01302 400 218

www.atlassecurity.services