



INFORMATION SECURITY POLICY

Company: P&R Fabrics Ltd

Registered Site Address: Hunter House, Holloway Drive, Wardley Industrial Estate, Manchester, M28 2LA

Policy Owner: Managing Director

Approved By: Senior Management

Effective Date: 6 Jan 2026

Review Date: Annually

1. Policy Statement

P&R Fabrics Ltd, operating from **Hunter House, Holloway Drive, Wardley Industrial Estate, Manchester, M28 2LA**, is committed to protecting the confidentiality, integrity, and availability of all information assets under its control. Information is a valuable business asset and must be protected from unauthorized access, disclosure, alteration, loss, theft, or destruction.

This policy establishes the framework for safeguarding information and ensuring compliance with legal, regulatory, contractual, and business requirements.

2. Purpose

The purpose of this policy is to:

- Protect company information and systems.
 - Reduce the risk of security incidents.
 - Support business continuity.
 - Ensure compliance with applicable legislation and regulatory requirements.
 - Protect customer, supplier, employee, and business data.
 - Define responsibilities for information security.
-

3. Scope

This policy applies to:

- All employees, directors, contractors, consultants, temporary workers, and agency staff employed or engaged by P&R Fabrics Ltd.
 - All activities conducted at the company's site located at **Hunter House, Holloway Drive, Wardley Industrial Estate, Manchester, M28 2LA.**
 - All information, whether held electronically, verbally, visually, or in paper format.
 - All company-owned or authorised systems, software, devices, networks, cloud services, and communications infrastructure.
-

4. Information Security Objectives

P&R Fabrics Ltd aims to:

1. Maintain the confidentiality of sensitive information.
 2. Preserve the integrity, accuracy, and completeness of information.
 3. Ensure information is available when required by authorised personnel.
 4. Prevent unauthorised access to company systems and data.
 5. Meet all applicable legal, regulatory, and contractual obligations.
 6. Continually improve information security processes and controls.
-

5. Roles and Responsibilities

Management Responsibilities

Management shall:

- Support and promote information security throughout the organisation.
- Provide adequate resources to implement appropriate controls.
- Review information security risks and incidents.
- Approve and maintain relevant policies and procedures.

Employee Responsibilities

All employees shall:

- Comply with this policy and related procedures.
- Protect company information assets.
- Report actual or suspected security incidents immediately.
- Complete any required information security awareness training.
- Use company systems responsibly and professionally.

6. Access Control

Access to company information and systems shall be granted on a business need-to-know basis.

The company will:

- Issue unique user accounts.
- Apply role-based access controls.
- Remove access promptly when employment or contracts end.
- Conduct periodic user-access reviews.
- Adopt the principle of least privilege.

Users must never:

- Share passwords.
 - Allow others to use their accounts.
 - Attempt to bypass security controls.
-

7. Password and Authentication Requirements

Users shall:

- Use passwords with a minimum length of 12 characters.
- Include a combination of letters, numbers, and symbols.
- Keep passwords confidential.
- Change passwords immediately if compromise is suspected.

Where available, Multi-Factor Authentication (MFA) will be implemented for enhanced protection.

8. Acceptable Use of Information Technology

Company systems and equipment are provided primarily for business use.

Users shall:

- Follow company procedures.
- Protect devices from theft, damage, and misuse.
- Lock devices when unattended.
- Use only authorised software and applications.

Users shall not:

- Download or install unauthorised software.
 - Engage in illegal or inappropriate activities.
 - Access content that may damage the reputation of the company.
 - Deliberately introduce malware or other malicious software.
-

9. Data Protection and Privacy

P&R Fabrics Ltd will process personal data in accordance with applicable UK data protection legislation.

Personal data shall be:

- Processed lawfully, fairly, and transparently.
 - Used only for legitimate business purposes.
 - Kept secure and accurate.
 - Retained only for as long as necessary.
 - Securely destroyed when no longer required.
-

10. Device and Endpoint Security

Company devices shall:

- Be password protected.
- Be maintained with current security updates.
- Use approved antivirus or endpoint protection software.
- Be encrypted where appropriate.

Any lost, stolen, or compromised device must be reported immediately.

11. Email and Internet Security

Employees shall:

- Exercise caution when receiving unexpected emails.
- Verify unusual requests involving payments, passwords, or sensitive information.
- Report phishing attempts immediately.

Sensitive information should only be transmitted using approved and secure methods.

12. Remote Working

Employees working remotely shall:

- Use secure internet connections.
 - Protect company information from unauthorised access.
 - Follow the same security standards required within company premises.
 - Use company-approved systems and equipment wherever possible.
-

13. Backup and Recovery

The company will maintain appropriate backup arrangements to protect critical business information.

Backups shall be:

- Performed regularly.
 - Protected from unauthorised access.
 - Tested periodically to verify successful restoration.
 - Retained in accordance with business requirements.
-

14. Physical Security

Appropriate physical security measures shall be maintained at:

Hunter House, Holloway Drive, Wardley Industrial Estate, Manchester, M28 2LA

Measures include:

- Controlled building access.
 - Visitor management procedures.
 - Secure storage of confidential information.
 - Clean desk and clear screen practices.
 - Secure disposal of confidential documents and records.
-

15. Information Security Incident Management

All information security incidents or suspected incidents must be reported immediately to management.

Examples include:

- Data breaches.
- Malware infections.
- Unauthorised access.
- Loss or theft of equipment.
- Phishing attacks.
- Accidental disclosure of confidential information.

All incidents will be investigated and appropriate corrective actions implemented.

16. Third-Party Security

Suppliers, contractors, and service providers that have access to company information or systems must maintain adequate security controls.

P&R Fabrics Ltd shall assess and manage risks associated with third-party relationships.

17. Compliance

Compliance with this policy is mandatory.

Failure to comply may result in:

- Disciplinary action.
 - Removal of system access.
 - Termination of employment or contract.
 - Legal action where appropriate.
-

18. Policy Review

This policy shall be reviewed annually or following any significant changes to:

- Business operations.
 - Technology systems.
 - Legal or regulatory requirements.
 - Information security risks.
-

DOCUMENT CONTROL

Policy Title: Information Security Policy

Company: P&R Fabrics Ltd

Site Address: Hunter House, Holloway Drive, Wardley Industrial Estate, Manchester, M28 2LA

Version: 1.0

Issue Date: 6 Jan 2026

Review Date: 6 Jan 2027

Approved By: Managing Director

Approval

I confirm that this policy has been approved and is supported by senior management.

Signed: 

Name: Malcolm Macleod

Position: Managing Director

Date: 6 Jan 2026

P&R Fabrics Ltd is committed to protecting its information assets and maintaining the highest practical standards of information security across all business operations conducted from Hunter House, Holloway Drive, Wardley Industrial Estate, Manchester, M28 2LA.