POLICY NAME:	DATA SECURITY	DATE:	JANUARY 2026
POLICY REVISION:	02	BY	JONATHAN CLARK
REVIEW PERIOD:	ANNUALLY	REVIEW:	JANUARY 2027

DATA SECURITY POLICY

CONTENTS

1. AMENDMENTS AND UPDATES

ISSUE	DATE	AMENDMENT / CHANGE
FIRST	Unknown	All previous versions saved in 'Archive' server
02	Jan 2026	Template, wording and sections, part of GFS improvement process.

2. PURPOSE

Glass and Framing Solutions Limited is committed to protecting the confidentiality, integrity, and availability of all its information assets. We recognise that effective data security is essential for maintaining the trust of our employees, clients, partners, and stakeholders.

This Data Security Policy outlines our dedication to implementing comprehensive security measures to safeguard sensitive information from unauthorised access, disclosure, alteration, or destruction. Our goal is to comply with all relevant data protection regulations while uploading the highest standards of data privacy and information security within the Company.

To assist us in this effort, we work with a specialised data security partner, Ability IT, who provides expert guidance and management of our data security practices.

3. SCOPE

This policy applies to all Glass and Framing Solutions Limited employees, contractors, consultants, temporary staff, and third-party partners who interact with the Company's data and information systems. It covers all forms of data including digital, physical, and archived information, and encompasses a wide range of data types, such as client data, employee records, financial details, intellectual property, project documentation, and supplier information.

4. POLICY STATEMENTS - DATA CLASSIFICATION

To ensure proper handling and protection, all data at Glass and Framing Solutions Limited is classified into the following categories:

- **Confidential:** This includes highly sensitive information such as client details, financial records, employee personal data, intellectual property, project plans, and proprietary business strategies. Confidential data is given the highest level of security controls.
- **Restricted:** This covers internal information including standard operating procedures, internal communications, and project documentation. Access to restricted data is limited to authorised personnel with specific clearance.
- **Public:** Information intended for public dissemination, such as marketing materials, product brochures, and published reports.

Proper classification of data allows us to determine the necessary security measures, access controls, and handling procedures for each information category.

5. POLICY STATEMENTS - DATA ACCESS CONTROL

- **Principle of Least Privilege:** Access to data is strictly on a need-to-know basis. Employees are granted access only to data and systems essential to their job functions.
- **Access Permissions:** Access rights are regularly reviewed, especially when employees change roles, leave the Company, or when new data categories are created. The review process involves assessing current access levels and adjusting to mitigate risks.
- **Authentication:**
    - All systems require unique user IDs and passwords that adhere to strong password policies, including complexity requirements, expiration timelines, and restrictions for reuse.
    - Two-factor authentication (2FA) is mandatory for accessing sensitive systems including the Company intranet, databases containing confidential information, and remote access portals.

- **Monitoring and Logging:** Access to sensitive data is continuously monitored and logged. Unauthorized access attempts are automatically flagged for investigation by the IT department and AbiltyIT's security monitoring service.

6. POLICY STATEMENTS - DATA STORAGE AND HANDLING

- **Electronic Data:**
  - Confidential data is stored on secured servers managed by AbilityIT, using industry standard encryption for data at rest and in transit.
  - Regular encrypted backups of critical data are conducted and stored off-site to prevent data loss in the event of system failures or cyber incidents.
  - Personal devices (laptops, smartphones) used for business must have up-to-date antivirus software, firewalls, password protection, and full disk encryption. Employees are required to report lost or stolen devices immediately.
- **Physical Data:**
  - Physical documents containing confidential or restricted information are stored in locked cabinets or designated secure areas, with access strictly limited to authorised personnel.
  - Access logs for physical documents are maintained for accountability and audits.
  - Disposal of physical documents is performed through secure shredding services to prevent unauthorised recovery or reconstruction.

7. POLICY STATEMENTS - DATA TRANSMISSION

Confidential and sensitive information must be transmitted using secure communication channels, such as:

- Encrypted email services.
- Secure File Transfer Protocol (SFTP) for file exchanges.
- Virtual Private Networks (VPNs) for remote access to Company resources.

- **Data Sharing Guidelines:** Sharing of confidential information with external parties is prohibited unless a non-disclosure agreement (NDA) is in place, and only the minimum necessary information is shared.
- **Prohibited Practices:** Employees are strictly forbidden from transmitting Company data through persona email accounts, unencrypted USB drives, or public messaging platforms.

8. POLICY STATEMENTS - DATA RETENTION AND DISPOSAL

- **Data Retention:** Glass and Framing Solutions Limited retains data only for as long as it is needed to fulfil its intended purpose and to comply with legal, regulatory, and business requirements.
- **Regular Data Audits:** Annual data audits, facilitated by AbilityIT, are conducted to identify and securely dispose of data that is no longer required. This includes reviewing digital data, physical documents, and archived information.
- **Secure Disposal:**
  - **Digital Data:** Disposal involves securely wiping digital storage devices using approved software tools, ensuring data cannot be recovered.
  - **Physical Documents:** Hard copies of confidential information are shredded using certified secure shredding services.

9. POLICY STATEMENTS - INCIDENT REPORTING AND RESPONSE

- **Immediate Reporting:** Employees must immediately report any actual or suspected data security breaches, such as unauthorised access, data loss, or phishing attempts, to the IT department or designated Data Protection Lead (DPL). AbilityIT monitors security events in real-time to ensure rapid response to incidents.
- **Incident Response:**
  - Collaboration with the DPL and AbilityIT, will promptly investigate incidents, access the scope, mitigate damage, and implement corrective measures.
  - In the event of a data breach, Glass and Framing Solutions Limited will notify affected individuals and regulatory authorities as required by law.
- **Post-Incident Analysis:** After resolving an incident, a review is conducted to identify weaknesses in the security protocols, with recommendations for improvements to prevent recurrence.

10. POLICY STATEMENTS - TRAINING AND AWARENESS

- **Mandatory Training:** All employees undergo mandatory data security training upon joining Glass and Framing Solutions Limited, with annual refresher courses. Training covers data classification, secure handling practices, recognising phishing and social engineering attacks, and incident reporting procedures.
- **Continuous Awareness:** Regular awareness campaigns, including newsletters, posters, and email alerts, keep data security practices at the forefront of employees' minds.
- **Third-Party Training:** Contractors, consultants, and third-party partners are also required to complete data security training relevant to their access levels, ensuring they comply with Glass and Framing Solutions Limited standards.

11. POLICY STATEMENTS - COMPLIANCE AND MONITORING

- **Compliance:** Glass and Framing Solutions Limited, in partnership with AbilityIT, strictly adheres to the General Data Protection Regulation (GDPR), the Data Protection Act, and other relevant legislation.
- **Regular Audits:** Internal and external audits are regularly conducted to assess compliance with this policy, identify vulnerabilities, and recommend improvements. AbilityIT provides detailed reports and support in this process.
- **Non-Compliance Consequences:** Non-Compliance with this policy may result in disciplinary action, including termination of employment and potential legal action if warranted.

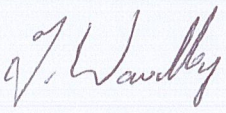
12. RESPONSIBILITIES

- **Employees:** Responsible for understanding and adhering to this policy, ensuring they handle data securely and report any security concerns immediately.
- **Managers:** Must ensure their teams comply with this policy, enforce access controls, and facilitate ongoing data security training.
- **IT Department:** Works with AbilityIT to implement technical security measures, monitor access logs, conduct regular security assessments, and respond to incidents.
- **Data Protection Lead (DPL):** Oversees compliance with data protection laws and this policy, manages data breaches, and serves as the point of contact for data security matters.

13. REVIEW AND CONTINUOUS IMPROVEMENT

This policy will be:

- Reviewed annually by Senior Management or more frequently if legislation or business operations change.
- Updated as necessary to ensure continued compliance and effectiveness.
- Supported by periodic audits and feedback mechanisms to identify and address potential weaknesses.

SIGNED:	
NAME:	Tony Waudby
TITLE:	Managing Director
SIGNED FOR:	Glass and Framing Solutions Limited
DATE:	15th January 2026