RETROSERVE LIMITED

Cyber Security policy

1. Governance, Accountability, and Regulatory Compliance

1.1 Policy Statement and Alignment

This Cyber Security and Data Protection Policy is mandatory for preserving the security, confidentiality, integrity, and availability (CIA Triad) of Retroserve Limited's information assets. Retroserve Limited adopts the technical and operational controls recommended by the National Cyber Security Centre's (NCSC) guidance, including the foundational principles of the **Cyber Essentials** scheme. Adherence to this policy is essential for maintaining our accredited status (CHAS Advanced, PAS 2030:2023, TrustMark) and ensuring strict compliance with UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018).

1.2 Scope and Applicability

This policy is mandatory for all Retroserve staff, contractors, and third-party vendors. It governs all company-owned assets (servers, networks, laptops, mobile devices) and all locations (offices, construction sites, and remote working environments).

1.3 Regulatory and Statutory Compliance

Retroserve is committed to the UK GDPR principle of explicit accountability. We are legally required to implement "appropriate technical and organisational measures" (ATO) to ensure data security, including encryption, system resilience, and the ability to restore access to personal data following an incident.

1.4 Roles and Responsibilities for Cyber Security

Executive Management holds ultimate accountability for defining and maintaining the cyber security strategy.

Role	Responsibility	Detailed Cyber Security Duty
Chief Executive Officer (CEO)	Ultimate Accountability & Risk Management Regime	Define the organization's overall Information Risk Regime, supported by the Board and senior managers.
Compliance & Operations Manager	Data Governance & Regulatory Reporting	Oversee GDPR adherence, execute the mandatory 72-hour regulatory breach notification process, and manage data subject requests.
IT Manager/Service Provider	Technical Implementation & Monitoring	Implement technical controls (MFA, firewalls, patching), maintain logging capabilities, manage data backups, and lead the technical response during incidents.

Department Managers	Access Approval & Training Compliance	Approve access requests based on job role (Least Privilege), ensure staff complete mandatory security awareness training, and manage remote working risks.
All Personnel	Incident Reporting & Policy Adherence	Strictly adhere to all policy provisions, report any suspected security threats or incidents immediately to the IT/Compliance Manager.

2. Information Asset Protection and Classification

2.1 Identifying Critical Data and Systems

Retroserve employs a continuous process to identify and inventory all critical digital assets. Security controls must be proportionate to the risk posed by unauthorized access or loss.

Data/System Type	**Data Classification**	**Justification and Security Objective**
Sensitive PII, HR, Financial Records	Restricted (Highest Protection)	Compromise poses severe financial, legal, and reputational harm (e.g., DPA 2018 fines). Security must be proportionate to the risk.
Proprietary Designs, IP, Client Contacts	Confidential	Loss undermines competitive advantage and requires stringent access control.
Core Operating Systems/Servers	Critical Infrastructure	Availability is paramount for operational continuity. Controls focus on resilience and immediate recovery.
Laptops and Mobile Devices	Endpoints	High risk due to portability; mandate Full Disk Encryption (FDE) and Remote Wipe capability.

2.2 Data Classification and Handling Protocols

- **Restricted Data Handling:** Mandatory Full Disk Encryption (FDE), mandatory Multi-Factor Authentication (MFA) for access, and Restricted Storage Locations must be enforced. Restricted data must not be stored on unencrypted removable media.
- **Confidential Data Sharing:** If emailed externally, documents must be encrypted and password-protected. The password must be sent via a secondary, trusted channel (e.g., phone call).

3. Technical Security Controls (Cyber Essentials Baseline)

Retroserve Limited uses the NCSC Cyber Essentials scheme as the baseline for technical security.

3.1 Authentication and Access Management

- **Multi-Factor Authentication (MFA) Mandate:** MFA is required wherever technically feasible. It is explicitly mandatory for: all remote access (VPN), all privileged/administrative accounts, and all systems handling Restricted or Confidential data. MFA should be implemented using methods that balance security and usability.
- **Strong Passwords:** All user passwords must be complex, using a minimum length of 12 characters, and passphrases are encouraged.
- **Principle of Least Privilege (PoLP):** Users are granted the minimal access rights necessary to perform their defined job function (Role-Based Access Control).

3.2 Network Security and Segmentation (Firewalls)

The IT Manager/Service Provider must ensure effective network security through firewalls and segmentation:

- **Firewall Management:** A security filter (firewall) must be created between the internet and the Retroserve network to deny traffic by default. Only necessary ports and protocols required by the devices in the networks should be allowed (allowed list principle).
- **Network Segmentation:** The network must be split into various segments. Sensitive devices and data, such as core servers and Restricted data archives, must be separated from general user devices and low-trust networks (like guest Wi-Fi).
- **Demilitarised Zone (DMZ):** Public-facing services (e.g., web or mail servers) must be kept in a separate, semi-trusted network zone (DMZ) to control and filter traffic between the internet and the internal sensitive networks.

3.3 System Maintenance and Malware Protection

- **Security Update Management:** The regular installation of security updates and patches across all company IT assets, including operating systems, anti-virus software, and specialized applications, is mandatory. Updates must be automatically enforced on mobile devices to remediate vulnerabilities.
- **Malware Protection:** Robust, up-to-date anti-virus/anti-malware solutions must be installed on all endpoints (laptops, mobile devices, servers) to identify and immobilise malicious software before it causes harm.

4. Data Resilience and Operational Security

4.1 Backup and Recovery Strategy

Retroserve maintains a mandatory Data Backup and Recovery Policy to support business continuity following a cyber incident, such as a ransomware attack.

- **Backup Strategy (3-2-1 Rule):** Critical data protection relies on the '3-2-1' rule:
    1. Maintain **3 copies** of data (original + two copies).

2. Store data on **2 different types** of media (e.g., local storage and cloud).
3. Keep at least **1 copy off-site** and logically isolated from the primary network to guarantee retrieval following a major cyberattack.

- **Recovery Testing:** Documented recovery procedures are mandatory, and testing must be performed regularly to ensure data can be restored accurately, reliably, and within defined timeframes.

4.2 Logging and Monitoring

Retroserve maintains robust logging capabilities as a core element of security monitoring and incident response.

- **Log Collection:** Systems are monitored and configured to collect logs of user activity, system events, access attempts, and security events.
- **Audit Trails:** Logging provides essential audit trails for understanding system usage, detecting unauthorized activity, and allowing retrospective analysis of security events to determine the impact of an incident.

5. Supply Chain and Third-Party Risk Management

Retroserve Limited must manage cyber risks associated with external suppliers, contractors, and managed service providers (MSPs).

- **Supplier Assessment:** A strategic approach to Cyber Supply Chain Risk Management (C-SCRM) must be adopted. Before contracting, Retroserve must define and communicate clear cyber security requirements to suppliers and verify their compliance.
- **MSP Certification:** When selecting MSPs to deliver IT services or manage data, Retroserve must prioritise providers with recognised security certifications, such as **Cyber Essentials Plus** or ISO 27001.
- **Contractual Clauses:** Contracts with third parties must include specific clauses relating to cyber security, incident notification, and the management of compliance.

6. Remote and Mobile Working Procedures

Home and mobile working, particularly for field staff using portable devices on construction sites, presents heightened risks of theft and data interception.

Threat Assessment Area	**Required Guidance and Control**
Data Interception Risk	All remote connections must exclusively use an approved Virtual Private Network (VPN). The VPN creates an encrypted tunnel, securing data over public Wi-Fi networks. MFA must be required for VPN access.
Device Theft/Loss Risk	Mandatory Full Disk Encryption (FDE) on all mobile devices (laptops/tablets) to protect data at rest. The capability to Remote Wipe a lost, stolen, or compromised device must be

	maintained (via MDM or similar service) „. Mobile devices shall be stored within a locked cabinet, desk, or room when not in use.
Malware Risk/Policy Enforcement	Staff must complete mandatory, regular training on spotting phishing attempts. Employees must not download non-approved applications onto devices connected to the network.
BYOD (Bring Your Own Device)	If personal devices are permitted, business data must be stored in a secure folder protected by a strong password. Overly sensitive (Restricted) information should be strictly restricted on BYOD.

7. Incident Response and Business Continuity

The Incident Response Plan (IRP) is structured to prioritize immediate containment, investigation, and adherence to regulatory reporting deadlines.

7.1 Incident Response Process and Timelines

Phase	Responsible Role	Key Action
Triage & Containment	IT Manager/Service Provider	Immediately isolate affected systems, halt malicious activity, and revoke unauthorized access to limit damage. Activate pre-defined emergency communication channels (if email is compromised).
Investigation & Eradication	IT Manager & Compliance Manager	Determine the scope of data compromised, eradicate all malicious software (virus, ransomware, etc.), and patch exploited vulnerabilities.
Restoration (Business Continuity)	IT Manager/Service Provider	Restore affected systems and data from verified, trusted backups within defined timeframes.
Regulatory Notification	Compliance Manager	Assess risk to individuals; if required, submit the Mandatory Data Breach Notification to the ICO within 72 hours of becoming aware of the breach.

7.2 Communication and Transparency

If a breach is likely to result in a high risk to the rights and freedoms of individuals, affected clients or employees must be promptly informed. The communication must clearly explain what happened, what specific data was affected, and what protective steps Retroserve is taking.

Signature: 
Full Name: Adam Shaid
Position: CEO
Date: 02/02/2025