jrhsupport

NETWORK SECURITY POLICY

NETWORK SECURITY POLICY

Policy Statement
JRH Support is committed to protecting its information assets, including client data, employee information, and proprietary business data, from unauthorised access, use, disclosure, disruption, modification, or destruction. This Network Security Policy outlines the rules and procedures for securing our network infrastructure and data. It helps us comply with data protection regulations (like UK GDPR) and maintain the trust of our clients.

Scope
This policy applies to all employees, contractors, and third parties who access or use JRH Support's network resources. It covers all network-connected devices, including computers, laptops, mobile devices, network equipment (routers, switches), wireless networks, and any cloud services utilised by the company.

General Security Principles
- **Confidentiality:** Only authorised individuals can access sensitive data.
- **Integrity:** Data remains accurate and complete, protected from unauthorised alteration.
- **Availability:** Network resources and data are accessible to authorised users when needed.
- **Least Privilege:** Users will only be granted the minimum access necessary to perform their job functions.
- **Accountability:** All network activities are traceable to individual users.

Network Access Control
JRH Support does not have it’s own Company network, but all staff access the Company scheduling software PASS for Care, which for the sake of this policy will be called the network.

1. **User Accounts and Passwords**

- All network users must have a unique user account.
- **Strong passwords** are mandatory:
    - Minimum 12 characters.
    - Mix of uppercase and lowercase letters, numbers, and symbols.
    - Not easily guessable (e.g., no personal information, common words).
    - Not reused from other accounts.
- Passwords must be changed every 90 days.
- Users must **never share their passwords**.
- Accounts of terminated employees or contractors must be disabled immediately upon their departure.

Network Devices and Configuration

2. **Firewalls**

- A **firewall** will be deployed at the network perimeter to control incoming and outgoing network traffic.
- Firewall rules will be configured to block unnecessary ports and services.
- Firewall logs will be regularly reviewed for suspicious activity.

3. **Wireless Networks (Wi-Fi)**

- Company Wi-Fi networks will be secured with **WPA2-Enterprise or WPA3 encryption**.
- Strong, complex passphrases will be used for Wi-Fi access.
- Network names (SSIDs) should not reveal sensitive information.

4. **Network Equipment (Routers, Switches)**

- Default passwords on all network equipment will be changed to strong, unique passwords immediately upon installation.
- Administrative interfaces for network devices will only be accessible from the internal network or via secure remote access.
- Firmware on network devices will be kept up to date.

Data Protection and Management

Data Encryption

- **Sensitive data, especially client records**, will be encrypted both in transit (e.g., using HTTPS for web access, VPN for remote connections) and at rest (e.g., full disk encryption on laptops, encrypted cloud storage).
- Where feasible, email containing sensitive information should be sent using secure, encrypted methods.

Data Backups

- **Regular backups** of all critical data will be performed.
- Backups will be stored securely, ideally off-site or in a secure cloud environment.
- Backup integrity will be tested periodically to ensure data can be restored.

Cloud Services

- All cloud services used by the company must be approved by management and assessed for their security compliance.

Multi-factor authentication (MFA) will be enabled for all cloud service accounts where available.

Software and Systems Security

Antivirus and Anti-Malware

- All computers connected to the network will have **up-to-date antivirus and anti-malware software** installed.
- Regular scans will be performed.

Software Updates and Patch Management

- Operating systems, applications, and network device firmware will be kept **up-to-date** with the latest security patches.
- Updates will be applied promptly after testing to address known vulnerabilities.

Software Installation

- Only **authorised software** may be installed on company devices.
- Users are prohibited from installing unapproved software or browser extensions.

Incident Response

- Any suspected network security incidents (e.g., unusual network activity, malware infection, unauthorised access attempts) must be reported immediately to the General Manager.
- An **Incident Response Plan** will be followed to contain, eradicate, and recover from security incidents.

Employee Responsibilities

- Adhere to all aspects of this Network Security Policy.
- Be vigilant about phishing attempts, suspicious emails, and unusual network behaviour.
- Lock computers when leaving their workstation unattended.
- Report any security concerns or incidents promptly.
- Attend mandatory security awareness training.

Policy Review

This Network Security Policy will be reviewed at least **annually**, or more frequently if there are significant changes in technology, business operations, or relevant regulations.

Enforcement

Violation of this policy may result in disciplinary action, up to and including termination of employment, and potentially legal action.

Paul Battershall
General Manager