WI-FI, NETWORK SECURITY AND PASSWORD MANAGEMENT POLICY

1. Policy Statement

National Workforce Ltd ("the Company") is committed to protecting its information, systems, networks, employees, customers, service users, suppliers and other stakeholders from cyber threats and unauthorised access.

The Company shall maintain appropriate technical and organisational measures to protect the **confidentiality, integrity and availability** of its information and information systems.

This policy establishes mandatory requirements for:

1. Wi-Fi and wireless network security;
2. wired and corporate network security;
3. remote network access;
4. passwords and authentication;
5. multi-factor authentication;
6. privileged and administrative accounts;
7. service and system credentials;
8. network-connected devices;
9. monitoring and logging;
10. incident reporting; and
11. access management.

The policy is designed to support National Workforce Ltd's obligations under applicable UK legislation and recognised cybersecurity good practice, including the UK GDPR, Data Protection Act 2018, NCSC guidance and Cyber Essentials.

The ICO states that organisations must use appropriate technical and organisational measures based on the nature and risks associated with their processing activities.

---

2. Scope

This policy applies to:

- All employees.
- Directors and officers.
- Contractors and temporary workers.
- Agency staff.
- Consultants.
- Volunteers and interns.
- Suppliers and third parties who are authorised to access Company systems.
- All Company offices and premises.
- All Company networks.
- Corporate Wi-Fi.
- Wired networks.
- VPN and remote-access services.
- Cloud services.
- Servers.
- Laptops and desktop computers.
- Mobile phones and tablets.
- Printers and multifunction devices.
- Network switches, routers, firewalls and wireless access points.
- IoT and other network-connected devices.
- User accounts.
- Administrator accounts.

- Service accounts.
- Application accounts.
- Database accounts.
- Cloud accounts.
- Any other system capable of authenticating a user or service.

The policy applies whether Company resources are accessed from Company premises, home, a customer's premises, a hotel, airport, public Wi-Fi, or another location.

---

3. UK Regulatory and Standards Alignment

This policy shall be implemented with regard to applicable requirements and guidance, including:

- UK GDPR, particularly the security principle and Article 32.
- Data Protection Act 2018.
- National Cyber Security Centre (NCSC) guidance.
- NCSC Cyber Essentials requirements.
- NCSC password guidance.
- Appropriate recognised information-security practices, including ISO/IEC 27001 principles where adopted by the Company.
- Contractual and customer security requirements applicable to National Workforce Ltd.

Cyber Essentials is a useful baseline, but the ICO notes that organisations may need controls beyond Cyber Essentials depending on their circumstances, processing activities and risk profile.

This policy is therefore intended to establish a broader internal standard rather than represent a statement that National Workforce Ltd is certified to any particular standard.

---

4. Security Principles

National Workforce Ltd shall apply the following principles.

4.1 Least Privilege

Users shall receive only the access required to perform their authorised duties.

4.2 Defence in Depth

Security shall not rely upon a single control. Appropriate combinations of authentication, encryption, network segmentation, endpoint security, monitoring and access controls shall be used.

4.3 Secure by Default

Systems shall be configured securely before being placed into production.

4.4 Zero Trust

Access shall not automatically be trusted simply because a user or device is connected to the corporate network.

4.5 Accountability

Individual users shall have identifiable accounts wherever technically possible. Shared accounts shall be avoided.

4.6 Risk-Based Security

Security controls shall be proportionate to the risks presented by the systems and information being protected.

---

5. Responsibilities

5.1 Board / Senior Management

Senior management shall:

- Approve this policy.
- Provide appropriate resources for cybersecurity.
- Ensure significant security risks are addressed.
- Review significant cybersecurity incidents.
- Support a culture of information security.

5.2 IT / Information Security

IT or the designated information-security function shall:

- Maintain secure network architecture.
- Configure and maintain firewalls.
- Manage Wi-Fi security.
- Manage authentication systems.
- Implement appropriate MFA.
- Manage privileged access.
- Maintain network and device inventories.
- Monitor security events.
- Manage vulnerabilities and security updates.
- Investigate security incidents.
- Maintain appropriate technical standards supporting this policy.

5.3 Managers

Managers shall:

- Ensure employees understand their security responsibilities.
- Approve access based on business need.
- Notify IT promptly of starters, leavers and role changes.
- Review access where appropriate.

5.4 Users

Users shall:

- Protect their credentials.
- Use only authorised systems and networks.
- Follow this policy.
- Report suspected security incidents immediately.
- Never share passwords.
- Never deliberately bypass security controls.

---

6. Corporate Wi-Fi Security

6.1 Approved Wireless Networks

Only Company-approved wireless networks may be used for normal Company business.

Corporate Wi-Fi shall be configured and managed by authorised IT personnel.

Unauthorised wireless access points, routers or hotspots must not be connected to the corporate network.

6.2 Wireless Encryption

Corporate wireless networks shall use modern security protocols.

WPA3-Enterprise should be the preferred standard where supported.

Where WPA3-Enterprise is not technically available, **WPA2-Enterprise using strong encryption** may be used where appropriately configured.

Legacy protocols such as WEP shall not be used.

6.3 Enterprise Authentication

Where technically practicable, corporate Wi-Fi shall use individual authentication through an enterprise authentication mechanism such as 802.1X/RADIUS.

Individual authentication is preferred over a single shared Wi-Fi password because it enables access to be attributed to an individual and removed when that individual's access ends.

6.4 Guest Wi-Fi

Guest Wi-Fi shall be logically separated from the Company's internal network.

Guest users must not have direct access to:

- Internal servers.
- Corporate workstations.
- Internal databases.
- Network-management systems.
- Administrative interfaces.
- Other restricted Company resources.

Guest access credentials shall be managed securely and changed when required by risk or suspected compromise.

6.5 Wireless Network Names

Corporate SSIDs shall not unnecessarily disclose sensitive technical information.

IT shall maintain a documented inventory of authorised SSIDs.

6.6 Wi-Fi Passwords

Where a shared Wi-Fi key is technically necessary, it shall:

- Be long and randomly generated.
- Not contain predictable Company information.
- Not be reused for unrelated systems.
- Be securely distributed.
- Be changed following suspected compromise.

---

7. Public and Untrusted Wi-Fi

Public Wi-Fi shall always be treated as an **untrusted network**.

Employees using public Wi-Fi shall:

- Verify the network name where possible.
- Avoid transmitting sensitive information over unprotected connections.
- Use the Company-approved VPN or secure access mechanism where required.
- Ensure device firewalls remain enabled.
- Ensure endpoint security remains active.
- Avoid connecting to suspicious or unknown networks.

Users must not assume that a network is safe merely because it requires a password.

---

8. Personal Hotspots

Personal mobile hotspots may be used only where reasonably necessary and where doing so does not circumvent Company security controls.

Employees shall:

- Secure their hotspot with a strong password.
- Keep their device's operating system and security software current.
- Use the Company's approved VPN or secure access mechanism where required.
- Disconnect when the business activity is complete.

---

9. Wired Network Security

Corporate wired networks shall be protected through appropriate:

- Network segmentation.
- Switch security.
- Firewall controls.
- Authentication.
- Access controls.
- Monitoring.
- Secure configuration.

Unauthorised network devices shall not be connected to Company network ports.

Where technically practicable, unused network ports shall be disabled or otherwise secured.

---

10. Network Segmentation

National Workforce Ltd shall use network segmentation where appropriate to reduce the impact of a compromise.

Segmentation should be considered for:

- Corporate user devices.
- Servers.

- Administrative systems.
- Guest networks.
- Printers.
- IoT devices.
- Voice systems.
- Security infrastructure.
- Sensitive applications.

Network access between segments shall be limited to authorised traffic.

---

11. Firewall Security

Firewalls shall protect appropriate boundaries between:

- The internet and Company networks.
- Internal network segments.
- Guest and corporate networks.
- Other environments requiring separation.

Firewall rules shall:

- Be based on business requirements.
- Follow least privilege.
- Be documented where appropriate.
- Be reviewed periodically.
- Remove obsolete rules.
- Be monitored for significant security events.

Internet-facing services shall be minimised.

---

12. Remote Access and VPN

Remote access to Company systems shall use approved technologies.
Where a VPN is required, employees must use the Company-approved VPN.
Remote-access services shall use strong authentication and MFA where technically supported and appropriate.
Employees shall not install or use unauthorised remote-access tools to bypass Company controls.

---

13. Password Management Policy

13.1 Mandatory Requirement

Every system that uses password-based authentication shall require an appropriate password or passphrase and shall implement controls against password guessing and compromise.

No employee may deliberately weaken or circumvent a system's authentication requirements.
The Company's password standard shall meet or exceed applicable NCSC and Cyber Essentials requirements.

---

14. Minimum Password Length

National Workforce Ltd shall adopt the following internal minimum standards:

Standard user accounts
Minimum: 14 characters.
Privileged / administrator accounts
Minimum: 16 characters.
Service and application accounts

Credentials shall be sufficiently strong and preferably randomly generated. Where supported, managed identities, certificates, keys or other non-password authentication mechanisms should be used.
The Company shall not impose an arbitrary maximum password length. NCSC guidance specifically advises against artificial maximum limits.
Where a legacy application cannot meet these requirements, IT shall document the exception and implement appropriate compensating controls.

---

15. Password Complexity

National Workforce Ltd shall **not rely primarily on arbitrary complexity rules**, such as requiring users to combine upper-case letters, lower-case letters, numbers and symbols in every password.

Instead, users shall be encouraged and supported to use:

- Long passwords.
- Passphrases.
- Multiple unrelated words.
- Password-manager-generated passwords.
- Unique passwords for each service.

NCSC guidance states that complexity requirements do not provide an effective defence against common attack methods and recommends minimum length and technical controls instead.

---

16. Common and Compromised Passwords

Where technically supported, systems shall prevent users from selecting passwords that are:

- Commonly used.
- Easily guessed.
- Known to have been compromised.
- Based on Company information.
- Based on usernames.
- Based on predictable keyboard patterns.

The NCSC Cyber Essentials requirements specifically recognise either MFA, a minimum 12-character password, or a shorter minimum combined with automatic blocking of common passwords as acceptable technical approaches for password-based authentication.

National Workforce Ltd's 14-character standard is therefore intended to provide an additional internal baseline.

---

17. Password Uniqueness

Passwords must be unique.

Employees shall **never reuse their National Workforce Ltd password** for:

- Personal email.
- Online banking.
- Social media.
- Shopping websites.
- Personal cloud services.
- Other employers.
- Any unrelated external service.

If one credential is compromised, password reuse can expose multiple systems.

---

18. Password Managers

National Workforce Ltd shall encourage or provide an approved password-management solution where appropriate.

Employees should use the approved password manager to:

- Generate unique passwords.
- Store passwords securely.
- Avoid password reuse.
- Generate high-entropy credentials.
- Share credentials only through authorised secure mechanisms where sharing is genuinely necessary.

Passwords must not be stored in:

- Unencrypted spreadsheets.
- Word documents.
- Plain-text files.
- Email.

- Sticky notes.
- Unsecured messaging applications.

---

19. Password Sharing

Passwords must never be shared.

Employees must not:

- Tell colleagues their password.
- Email passwords.
- Send passwords by SMS or chat.
- Write passwords where unauthorised people can see them.
- Allow another person to use their account.

IT personnel shall not request a user's complete password.

Where multiple people require access to the same resource, an approved delegated-access, shared-vault, service-account or privileged-access mechanism shall be used.

---

20. Password Changes

Passwords shall be changed immediately when:

- Compromise is suspected.
- A password has been disclosed.
- A phishing attack may have captured the credential.
- An unauthorised person may have obtained access.
- IT/security instructs the user to change it.
- A system-specific risk or contractual requirement requires a change.

National Workforce Ltd shall not require routine password changes at arbitrary intervals solely for the sake of changing passwords where there is no evidence of compromise, unless a specific system, contractual or regulatory requirement requires this.

---

21. Failed Authentication Attempts

Systems shall use appropriate technical controls to resist brute-force attacks.

Depending on the system, controls may include:

- MFA.
- Rate limiting.
- Login throttling.
- Progressive delays.
- Account/device lockout.
- Monitoring and alerting.

Systems shall be configured so that password guessing is appropriately restricted.

Current Cyber Essentials requirements state that password authentication should be protected against brute-force guessing and, where throttling is used, should not allow more than 10 guesses in five minutes.

---

22. Multi-Factor Authentication

MFA shall be implemented for systems where it is available and appropriate to the risk.

MFA shall be prioritised for:

- Email.
- Cloud services.
- VPN.
- Remote access.
- Administrator accounts.
- Financial systems.
- Systems containing personal data.
- Systems containing commercially sensitive information.

Where technically and operationally feasible, phishing-resistant methods such as passkeys or security keys should be preferred for higher-risk access.
Employees must not approve an unexpected MFA request.
Repeated unexpected MFA prompts must be reported to IT/security.

---

23. Administrator and Privileged Accounts

Administrators shall use separate privileged accounts for administrative activities.
Privileged accounts shall:

- Have unique credentials.
- Use MFA where available.
- Be restricted to authorised personnel.
- Be monitored appropriately.
- Be reviewed periodically.
- Have only the permissions necessary.

Administrators should not use privileged accounts for ordinary email, web browsing or general-purpose activities.

---

24. Service Accounts

Service accounts shall:

- Have a defined owner.
- Have a documented purpose.
- Have only necessary privileges.
- Use unique credentials.
- Be reviewed periodically.
- Be disabled when no longer required.

Static passwords should be avoided where secure alternatives such as managed identities or certificates are available.
Credentials must not be hard-coded into publicly accessible source code.

---

25. Default Credentials

All default passwords and credentials must be changed or disabled before systems are placed into operational use.
This applies to:

- Routers.
- Switches.
- Firewalls.
- Wireless access points.
- Printers.
- Servers.
- Applications.
- IoT equipment.
- Cloud services.
- Other network-connected devices.

NCSC guidance specifically recommends changing default passwords because default credentials can make compromise significantly easier.

---

26. Device Security

Company-managed devices shall use appropriate security controls, including:

- Supported operating systems.
- Security updates.
- Endpoint protection.

- Host firewall.
- Disk encryption where appropriate.
- Secure screen locking.
- Central management where appropriate.
- Secure configuration.

Users must not disable security software or security controls without IT authorisation.

---

27. Network Equipment

Routers, switches, firewalls and wireless access points shall:

- Run supported firmware.
- Have default credentials removed or changed.
- Restrict management interfaces.
- Use secure management protocols.
- Be appropriately monitored.
- Be securely configured.
- Have configuration backups where appropriate.

Administrative access to network infrastructure shall be restricted to authorised IT personnel.

---

28. Encryption

Appropriate encryption shall be used to protect sensitive information in transit and at rest where the risk warrants it.

Sensitive information should not be transmitted using insecure, unencrypted protocols where a secure alternative is available.

Examples of secure technologies include appropriately configured:

- HTTPS.
- TLS.
- SSH.
- SFTP.
- VPN.
- Secure cloud services.

The ICO recognises encryption as an important technical measure where appropriate to the risks associated with personal information.

---

29. Network Monitoring and Logging

Appropriate security logging shall be implemented based on risk.

Logs may include:

- Authentication attempts.
- Successful and failed logins.
- Administrative activity.
- VPN access.
- Firewall events.
- Wireless authentication.
- Security alerts.
- Significant configuration changes.

Logs shall be protected against unauthorised alteration and access.

Monitoring shall be conducted in accordance with applicable law and Company privacy requirements.

---

30. Vulnerability and Patch Management

IT shall maintain appropriate processes for:

- Identifying vulnerabilities.
- Assessing risk.

- Applying security updates.
- Replacing unsupported systems.
- Tracking remediation.

Internet-facing and critical systems shall receive priority.
Unsupported software shall be removed, upgraded, isolated or protected with appropriate compensating controls.

---

31. Access Control

Access shall be:

- Authorised.
- Business justified.
- Based on least privilege.
- Individually attributable where possible.
- Reviewed periodically.

Access rights shall be amended promptly when an employee changes role.
Access shall be removed promptly when an employee, contractor or supplier no longer requires access.

---

32. Joiners, Movers and Leavers

Joiners

New employees shall receive only the access required for their role.

Movers

When an employee changes role, previous access shall be reviewed and removed where no longer required.

Leavers

When employment or engagement ends:

- Accounts shall be disabled promptly.
- Remote access shall be revoked.
- VPN access shall be removed.
- Privileged access shall be removed.
- Company devices shall be recovered.
- Company credentials shall no longer be available to the individual.

---

33. Personal Devices / BYOD

Personally owned devices may access Company systems only where explicitly authorised.
Authorised devices shall meet Company security requirements.
Depending on risk, requirements may include:

- Supported operating system.
- Security updates.
- Device encryption.
- Screen lock.
- MFA.
- Mobile/device management.
- Ability to remove Company information.

The Company may block access from devices that do not meet security requirements.

---

34. Third-Party Access

Third parties shall receive only the access necessary to perform authorised services.
Where appropriate:

- Individual accounts shall be used.
- MFA shall be required.
- Access shall be time-limited.
- Supplier access shall be reviewed.

- Unused accounts shall be disabled.
- Security obligations shall be incorporated into contractual arrangements.

Where third parties process personal data on behalf of National Workforce Ltd, appropriate contractual and security arrangements shall be maintained. The ICO notes that processor contracts should require appropriate Article 32 security measures.

---

35. Phishing and Credential Theft

Employees shall remain alert to attempts to steal passwords or authentication information.

Examples include:

- Fake IT-support messages.
- Fake password-reset requests.
- Unexpected MFA requests.
- Fake Microsoft/Google login pages.
- Requests for passwords.
- Urgent requests for confidential information.
- Suspicious attachments or links.

Employees must report suspected phishing immediately.

If a password may have been compromised, the employee shall:

1. Report the incident to IT/security.
2. Change the affected password using an approved method.
3. Change any other account using the same password.
4. Follow instructions provided by IT/security.

---

36. Security Incident Reporting

Employees must immediately report:

- Lost or stolen Company devices.
- Compromised passwords.
- Unauthorised access.
- Suspicious login notifications.
- Unexpected MFA requests.
- Malware.
- Ransomware.
- Suspicious Wi-Fi activity.
- Unauthorised network devices.
- Phishing attacks.
- Accidental disclosure of credentials.
- Suspected data breaches.

Employees must not deliberately conceal a security incident.

---

37. Security Awareness Training

All personnel shall receive appropriate security awareness training.

Training shall cover:

- Password security.
- MFA.
- Phishing.
- Wi-Fi security.
- Public Wi-Fi.
- Social engineering.
- Device security.
- Data protection.
- Incident reporting.

- Safe remote working.

Personnel with administrative privileges shall receive additional technical security training appropriate to their responsibilities.

---

38. Business Continuity and Recovery

National Workforce Ltd shall maintain appropriate measures to support the availability and recovery of critical systems.

Where appropriate, this shall include:

- Backups.
- Recovery procedures.
- Resilient network infrastructure.
- Incident-response procedures.
- Disaster-recovery arrangements.
- Regular testing.

The ICO identifies resilience and the ability to restore access and availability following an incident as important elements of appropriate security measures.

---

39. Data Protection

Where Company networks or systems process personal data, appropriate technical and organisational measures shall be implemented in accordance with applicable data-protection requirements.

Security controls shall consider:

- The type of information processed.
- The sensitivity of the information.
- The likelihood of attack.
- The potential impact of compromise.
- The state of available technology.
- Implementation costs.
- Business requirements.

The Company shall periodically review whether security controls remain appropriate.

---

40. Prohibited Activities

Users must not:

- Attempt unauthorised access.
- Bypass authentication.
- Disable security controls.
- Install unauthorised network equipment.
- Conduct unauthorised vulnerability scanning.
- Intercept communications without authorisation.
- Share credentials.
- Use another person's account.
- Introduce malware.
- Attempt to circumvent network restrictions.
- Connect unauthorised devices to the corporate network.
- Use Company systems for unlawful activities.

---

41. Exceptions

Any exception to this policy must be:

1. Documented.
2. Business justified.
3. Risk assessed.
4. Approved by the appropriate authority.

5. Time limited where practical.
6. Reviewed periodically.

Where a technical limitation prevents compliance, IT shall implement appropriate compensating controls.

---

42. Compliance and Enforcement

Compliance with this policy is mandatory.

Failure to comply may result in:

- Removal of system access.
- Additional security restrictions.
- Formal disciplinary action.
- Contractual action against suppliers or contractors.
- Referral to law enforcement or regulators where legally appropriate.

The Company shall apply disciplinary measures consistently and proportionately.

---

43. Audit and Review

National Workforce Ltd shall periodically review compliance with this policy.

Reviews may include:

- Password configuration reviews.
- MFA coverage.
- Network configuration reviews.
- Wi-Fi security reviews.
- Firewall reviews.
- Privileged-access reviews.
- Vulnerability assessments.
- Security audits.
- Log reviews.
- User-access reviews.

The policy shall be reviewed at least annually and following:

- Significant cybersecurity incidents.
- Material technology changes.
- Significant changes in business operations.
- Relevant changes to UK legislation or regulatory guidance.
- Significant changes to the threat environment.

---

44. Minimum Security Baseline

Security Area	National Workforce Ltd Requirement
Standard user password	Minimum 08 characters
Privileged password	Minimum 16 characters
Password maximum	No arbitrary maximum
Password reuse	Prohibited
Password sharing	Prohibited
Common passwords	Must be prevented where technically supported
Default passwords	Must be changed or disabled
MFA	Required where available and appropriate
Corporate Wi-Fi	WPA3-Enterprise preferred
WPA2	WPA2-Enterprise permitted where necessary
WEP	Prohibited
Guest Wi-Fi	Must be separated from corporate network

Public Wi-Fi	Treated as untrusted
Remote access	Approved secure mechanism
Administrator accounts	Separate privileged accounts
Service accounts	Unique, controlled and documented
Network segmentation	Required where justified by risk
Firewall	Required at appropriate network boundaries
Security updates	Risk-based and timely
Encryption	Used where appropriate to risk
Access	Least privilege
Security incidents	Report immediately
Default credentials	Must not remain in production
Unsupported systems	Must be replaced, isolated or otherwise mitigated
Policy exceptions	Must be formally approved

---

45. Employee Security Responsibilities

Every employee and authorised user shall:

- Keep passwords confidential.
- Use unique passwords.
- Use MFA when required.
- Lock devices when unattended.
- Use only authorised networks.
- Avoid sensitive activity on untrusted Wi-Fi unless appropriate security protections are in place.
- Report suspected compromise immediately.
- Follow IT security instructions.
- Complete required security training.
- Protect Company equipment and information.

Appendix A – Employee Password Rules

Employees shall remember the following:

1. Use a long password or passphrase.
2. Use a different password for every important account.
3. Never share your password.
4. Never reuse your Company password elsewhere.
5. Use the approved password manager where provided.
6. Never approve an unexpected MFA request.
7. Never enter a password into a suspicious link or website.
8. Report suspected password compromise immediately.
9. Never write passwords where other people can see them.
10. Contact IT if you are unsure whether a login or password request is legitimate.

Appendix B – Wi-Fi Rules for Employees

Employees shall:

1. Use Company-approved Wi-Fi for Company business where available.
2. Treat public Wi-Fi as untrusted.
3. Use the approved VPN when required.
4. Do not connect unknown devices to the corporate network.

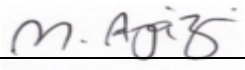
5. Do not create unauthorised wireless access points.
6. Do not share corporate Wi-Fi credentials unnecessarily.
7. Report suspicious wireless activity to IT.
8. Keep laptops and mobile devices updated.
9. Keep firewalls and endpoint security enabled.
10. Report lost or stolen devices immediately.

Appendix C – Policy References

This policy should be read alongside National Workforce Ltd's:

- Information Security Policy.
- Acceptable Use Policy.
- Data Protection Policy.
- Incident Response Procedure.
- Remote Working Policy.
- Access Control Policy.
- Business Continuity Policy.
- Data Retention Policy.
- Bring Your Own Device Policy.
- Supplier Security Policy.

External guidance used in developing this policy includes current NCSC Cyber Essentials requirements and NCSC password guidance, together with ICO guidance concerning UK GDPR security obligations.

Signed:  Position: Managing Director Date: 01/04/2026