# Cybersecurity Policy for The North West Aerospace Alliance

**Effective Date:** 26/06/2024

**Next Review Date:** 25/06/2025


---

## 1. Introduction and Purpose

The **North West Aerospace Alliance (NWAA)** is committed to protecting its information systems, sensitive data, and technological infrastructure from cyber threats and vulnerabilities. The purpose of this Cybersecurity Policy is to define and establish cybersecurity practices that ensure the confidentiality, integrity, and availability of all digital resources within the NWAA.

- **This policy is designed to:**
  **Introduction and Purpose**: The policy aims to safeguard data, minimise cyber risks, and ensure compliance with cybersecurity regulations and best practices.
- **Scope and Responsibilities**: The policy applies to all individuals with access to NWAA's systems, outlining roles and responsibilities for executive leadership, IT security, employees, and the Incident Response Team.
- **Access Control and Data Protection**: Measures include user authentication, access rights based on job responsibilities, data encryption, regular backups, and secure data disposal.

- **Incident Response and Compliance**: NWAA has an incident response plan, communication protocols for cybersecurity incidents, and ensures compliance with legal and regulatory requirements..

---

## 2. Scope

This policy applies to all employees, contractors, third-party vendors, and any other individuals who have access to NWAA's information systems, networks, and data. It encompasses all devices, software, hardware, communications infrastructure, and any information exchanged across or stored in NWAA's systems.

---

## 3. Roles and Responsibilities

- **Executive Leadership:** The leadership team is responsible for overseeing the cybersecurity strategy, ensuring resource allocation, and ensuring the enforcement of this policy.
- **IT Security Team:** The team is responsible for implementing security measures, conducting regular security audits, and managing incident response activities.
- **Employees and Contractors:** All individuals are responsible for following security protocols, reporting suspicious activities, and adhering to the cybersecurity guidelines set forth in this policy.
- **Incident Response Team (IRT):** A designated team within NWAA will manage the detection, management, and resolution of cybersecurity incidents.

---

## 4. Access Control

- **User Authentication:** All users will be required to use strong passwords, and multi-factor authentication (MFA) will be enforced for accessing sensitive systems and data.
- **Access Rights:** Access to sensitive systems and data will be granted based on job responsibilities. Users will be assigned the least privilege necessary to perform their work.
- **Account Management:** Accounts will be created, modified, and deactivated based on user roles, and regular audits will ensure access is current and appropriate.
- **The business uses conditional access** to block all non-UK sign-in attempts, thereby reducing the risk of unauthorised access from overseas

---

## 5. Data Protection

- **Data Encryption:** Sensitive data will be encrypted both in transit and at rest, utilising industry-standard encryption protocols to prevent unauthorised access.

- **Data Backup:** NWAA will perform regular backups of critical data and store backup copies securely, ensuring the ability to recover from data loss or corruption.
- **Data Retention and Disposal:** Data will be retained only for the duration necessary for business purposes and in compliance with applicable laws. When data is no longer needed, it will be securely destroyed.

---

### 6. Network Security

- **Firewalls and Intrusion Detection Systems:** NWAA will deploy firewalls and intrusion detection systems (IDS) to monitor and block unauthorised access attempts to its networks.
- **VPN and Remote Access:** Secure Virtual Private Network (VPN) solutions will be used for remote access to NWAA's internal systems. All users working remotely must connect through the VPN.
- **Segmentation:** Sensitive data will be segmented from less critical data, reducing exposure in case of a breach.

---

### 7. Security Awareness and Training

- **Employee Training:** All employees, contractors, and partners will undergo regular cybersecurity training, including safe data managing practices, identifying phishing attacks, and secure use of devices.
- **Simulated Phishing Exercises:** NWAA will conduct simulated phishing campaigns periodically to assess employee awareness and response to phishing attempts.

---

### 8. Incident Response and Reporting

- **Incident Reporting:** Employees must immediately report any suspected cybersecurity incident, including phishing emails, malware, or unauthorised access, to the IT Security Team.
- **Incident Response Plan:** A comprehensive plan will be followed to respond to and manage cyber incidents, including containment, eradication, recovery, and forensic analysis.
- **Communication Protocols:** Clear protocols will be established for notifying relevant stakeholders, including affected members, about cybersecurity incidents when necessary.

---

### 9. Compliance and Legal Requirements

- **Regulatory Compliance:** NWAA is committed to complying with relevant legal and regulatory requirements, including the General Data Protection Regulation (GDPR), the Cybersecurity Act, and other applicable standards and frameworks.

- **Third-Party Risk Management:** When collaborating with third-party vendors, NWAA will ensure that cybersecurity standards are met, including the implementation of security controls and appropriate agreements for data protection.

---

### 10. Security Monitoring and Auditing

- **Auditing and Logging:** Logs of critical system and network activities will be kept for audit purposes. Regular reviews will be conducted to ensure compliance with security practices.

---

### 11. Mobile Device Security

- **Mobile Device Management (MDM):** All mobile devices used for work-related purposes must adhere to NWAA's Mobile Device Security Policy, including the use of MDM software to enforce security protocols.
- **BYOD (Bring Your Own Device):** Is strictly not permitted

---

### 12. Business Continuity and Disaster Recovery

- **Business Continuity Plan (BCP):** NWAA will ensure that critical business functions can continue in the event of a cyber incident or other disruptions.
- **Disaster Recovery Plan (DRP):** Procedures for restoring systems, data, and applications will be in place to ensure quick recovery following a cybersecurity breach or disaster.

---

### 13. Review and Policy Updates

- **Regular Review:** This Cybersecurity Policy will be reviewed at least annually, or more frequently if there are significant changes to the threat landscape or organisational needs.
- **Policy Enforcement:** Violations of the policy may result in disciplinary action, including termination of employment or contractual agreements, in accordance with NWAA's internal policies.

---

### 14. Conclusion

The **North West Aerospace Alliance (NWAA)** is committed to maintaining the highest standards of cybersecurity to protect its data, systems, and reputation. All members, employees, contractors, and stakeholders must comply with this policy to ensure the safety and integrity of NWAA's digital environment.

---

**Approved by:**
CEO North West Aeropace Alliance
Date: 01/12/2024