


<p style="text-align: center;">REGIONAL WIRELESS COOPERATIVE POLICIES AND PROCEDURES</p>	
	<p style="text-align: center;">No. S-04.11</p>
<p>Subject:</p> <p>Network Security Policy</p>	<p style="text-align: center;">Revised: 11/2024</p> <p style="text-align: center;">Prior Rev: 11/2022</p>

1.0 Purpose

1.1. The purpose of this policy is to establish the security requirements for the RWC Network.

2.0 Owner

2.1. RWC Operations Working Group (OWG).

3.0 Applies To

3.1. All users of the RWC network; including Members, agency personnel with RWC system equipment access, and approved service providers.

4.0 Background

4.1. The RWC Network is a public safety grade radio communications system comprised of hardware, software, and applications that directly support mission critical communications. The RWC Network shall be protected from cyber threats vulnerabilities and potential exploits by implementing security controls that prevent or mitigate potential cybersecurity risks that could result in disruptions or service outages.

5.0 Policy Statement

5.1. All users are to preserve the confidentiality, integrity, and availability of the RWC Network. Agency personnel that have access to the RWC infrastructure shall follow network security best practices, processes, procedures, and standards to protect the RWC Network from internal and external sources of harm. Information and security controls established by the RWC shall extend to all users, agency members, and contracted third-party manufacturers or service providers.

6.0 Supporting Rules

6.1. Asset Management

6.1.1. Inventories are maintained for physical devices, hardware, and software.

6.1.1.1. Assets will be prioritized based on classification, criticality, and value.

6.1.2. Removals, transfers, and disposition of physical devices must be formally managed including a process to remove surplus assets.

6.2. Risk Management

6.2.1. A risk management framework provides for setting objectives, principles for action, and sense of direction.

6.2.1.1. Ensure all risk management activities are conducted and implemented in a controlled manner.

6.2.1.2. Achieve a risk management capability that meets changing business needs and is appropriate in size and complexity for the radio network.

6.2.2. Risk assessment

6.2.2.1. Assets are weighted and documented to assess vulnerabilities, risks, and threats.

6.2.3. Risk Mitigation

6.2.3.1. Risks shall be mitigated based on four types which include: Acceptance, Avoidance, Limitation, and Transference.

6.3. Access Control

6.3.1. The radio network maintains physical access controls to identify, authenticate, and authorize personnel to secure or sensitive areas based on role and privileges assigned to the individual.

6.3.2. The radio network maintains a remote access policy to identify, authenticate, and authorize personnel to secure or sensitive areas based on role and privileges assigned to the individual.

6.4. Awareness & Training

6.4.1. End Users will complete annual cybersecurity awareness training that addresses social engineering, malware, virus, phishing, mobile device security, data handling, passwords & authentication, personnel roles, and response to breaches or compromised devices.

6.4.2. System administrators and Information Security personnel shall complete additional training that maintains the confidentiality, integrity, and availability of the network.

6.4.2.1. End user training records shall be maintained by Information Security personnel.

6.5. Data Security

6.5.1. The network shall utilize best practices for data-at-rest and data-in-transit.

6.5.1.1. The network will implement security controls such as firewalls, encryption, or network access controls to achieve data security.

6.5.2. Development and testing of applications, software, or traffic shall be kept separate from production applications, software, or traffic.

6.6. Configuration Change Control

6.6.1. Maintenance and repair activities for the network will be scheduled and managed through the RWC Network Operations Center (NOC) as a central point of management for on-site or remote maintenance.

6.6.1.1. All users including support personnel will follow RWC notification procedures for any maintenance being performed during business hours or after-hours.

6.7. System Devices

6.7.1. Any devices that are used to connect to the RWC Network, directly, will be protected for the purpose of supporting the RWC system. Support personnel are responsible for ensuring devices connected to the RWC Network have a current applicable end point security solution (e.g. antivirus, antimalware, firewalls).

6.7.2. Any media that is to be connected to RWC infrastructure, consoles, IP logging recorders or subscriber administrative terminals must first be scanned by an isolated computer that has an end point security solution.

6.8. Passwords follow National Institute of Standards and Technology (NIST) password guidelines at a minimum

6.8.1. Password length shall contain 15 characters or longer with a minimum of one uppercase, one number, and one special character.

6.8.2. Passwords must be protected and not shared with anyone without proper authorization.

6.8.3. User accounts will be created and managed by the RWC Network Operations Manager.

6.8.4. Multi-factor authentication shall be used when applicable.

6.9. Auditing

6.9.1. All users shall participate in scheduled audits to verify if the network is operating according to cybersecurity standards, regulations, and guidelines.

6.10. Monitoring

6.10.1. Anomalies and Events within the physical and network environments will be monitored by the NOC.

6.10.2. Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) shall be utilized to monitor for malicious activity or policy violations.

6.10.3. Vulnerability Scans shall be used to detect and classify system weaknesses along with analyzing any implemented countermeasures.

6.11. Breaches

6.11.1. The Network Operations Manager will refer to appropriate security breach procedures in mitigating identified issues.

6.12. Response and Recovery

6.12.1. The process of response planning will develop options and determine actions to reduce or eliminate threats to the system.

6.12.2. Information sharing shall occur at Operations Working Group (OWG) meetings, through status reports, or other strategic meetings.

6.12.3. Coordination with Stakeholders will occur by the RWC Executive Director or by the Network Operations Manager.

6.12.4. Response Analysis

6.12.4.1. Impacts of network events shall be understood to determine the appropriate response to the event.

6.12.4.2. Device forensics are performed to collect, process, preserve, and analyze computer-related evidence when applicable.

6.12.4.3. Incidents will be categorized in a response plan to address and manage any security breach or cyberattack.

6.12.5. Mitigation

6.12.5.1. Implementation of any mitigation strategy will refer to a verified response plan.

6.12.6. Improvements

6.12.6.1. Incident lessons learned may result in additional strategies to address security breaches or cyber-attacks.

6.12.7. Recovery planning

6.12.8. Restoration and communications

7.0 Responsibilities

7.1. The Network Operations Manager is responsible for the following practices relating to RWC network security:

7.1.1. Update end-point security solution software and server in compliance with Motorola network standards.

7.1.2. Monitor, identify, and maintain information related to RWC infrastructure and components regarding risks, threats, and vulnerabilities to the RWC.

- 7.1.3. Develop plans for minimizing or eliminating security-related problems, and any actions necessary for the implementation of the plans.
- 7.1.4. Use appropriate supporting organizations or approved contractors as required to maintain adherence to network security policies.
- 7.1.5. Provide reports to the OWG on the status of network security, potential threats and risks, and actions involved in protecting the RWC Network.
- 7.1.6. Shall have responsibility for ensuring that overall network security is consistent with current technology, and for ensuring that the RWC policies related to network security are followed.
- 7.1.7. User accounts will be created and managed by the RWC Network Operations Manager.

7.2. RWC Members and Users:

- 7.2.1. Responsible for ensuring approved users and service providers adhere to this policy.
 - 7.2.2. Shall use due diligence in the protection of the RWC Network infrastructure, network devices, peripherals, network resources and data.
 - 7.2.3. Any breaches in network security will immediately be reported to the RWC Network Operations Center (NOC) who shall take steps to minimize the danger to the operational capabilities of the RWC.
- 7.3. RWC Network Manager(s), users and approved service providers are responsible for monitoring network incursions, which may be introduced by external media or non-certified software that endangers the confidentiality, integrity, and availability of the network.

8.0 Conditions for Exemption or Waiver

- 8.1. As provided in the Waiver or Exception Policy.

9.0 Applicable Policies and/or Procedures

- 9.1. As listed at www.rwcaz.org.