MultiTech RED-DA Compliance Summary

Updated security response to the previous document: 09122024-001 September 24, 2024

Introduction

Multi-Tech Systems, Inc. (MultiTech) is committed to meeting the European Union's Radio Equipment Directive Delegated Act (RED-DA) 2022/30, which took effect on August 1, 2025. This regulation mandates cybersecurity requirements for internet-connected radio equipment under Articles 3.3 (d), (e), and (f) of Directive 2014/53/EU to safeguard networks, protect personal data, and prevent fraud. MultiTech's approach to compliance is to ensure its product portfolio provides secure, resilient, and trustworthy IoT solutions for the EU market.

Understanding RED-DA Requirements

RED (Directive 2014/53/EU) sets essential requirements for radio equipment sold in the EU, including safety, electromagnetic compatibility, and spectrum efficiency. RED-DA expands this to include cybersecurity for internet-connected devices, which applies to MultiTech's IoT gateways, modems, and routers.

Key Articles of RED-DA:

Article	Requirement	MultiTech Implementation
3.3 (d)	Network protection via secure authentication and access control	TLS, certificate-based access, firewall rules
3.3 (e)	Safeguarding personal data and privacy	Encryption, secure storage, user consent
3.3 (f)	Protection against financial fraud	Not applicable - MultiTech products do not process financial transactions

Compliance Standards

MultiTech aligns with and follows compliance standards EN 18031-1, EN 18031-2, and EN 18031-3 (published January 2025), which provide technical guidance for RED-DA conformity.

Scope of MultiTech Products

MultiTech's gateways, routers, and modems feature wired and wireless interfaces capable of autonomous internet connectivity and fall within the scope of RED-DA. Devices placed on the EU market before August 1, 2025, are exempt, but new units or major updates after this date must comply.

Why Compliance Matters

RED-DA compliance is critical for MultiTech to:

- Maintain uninterrupted EU market access
- Protect users from cybersecurity threats like unauthorized access, data breaches, and network disruptions (e.g., DDoS attacks)
- Enhance product trust and competitiveness

By aligning with EN 18031 standards, MultiTech ensures its IoT products meet EU expectations for network resilience, data privacy, and fraud prevention.

MultiTech Compliance Strategy

MultiTech assessed its products and deemed them RED-DA compliant. The compliance review included:

1. Product and Risk Assessment

- **Inventory:** Identify all in-scope products, including gateways, modems and routers with both wired and wireless connectivity
- **Assets:** Map network, security, and privacy assets like network interfaces, authentication mechanisms, and data storage to EN 18031 requirements
- **Risk:** Perform comprehensive risk assessments for vulnerabilities across network connectivity, data handling and transaction processes

2. Cybersecurity Controls

- **Network Protection (EN 18031-1):** Implement secure communication protocols like TLS encryption, robust certificate-based authentication, and access controls in MultiTech products
- **Data Privacy (EN 18031-2):** Incorporate encryption for data in transit and at rest, secure storage, and user consent mechanisms into product software
- **Fraud Prevention (EN 18031-3):** Not applicable - MultiTech products do not support financial transactions

3. Compliance Pathways

- **Self-Assessment:** Follow a self-assessment route for most MultiTech products to confirm EN 10831 compliance and prepare technical documentation to support a self-signed Declaration of Conformity (DoC)
- **Notified Body Engagement:** Engage Notified Bodies for EU-Type Examination Certificates (EU-TEC) to ensure compliance where appropriate

4. Lifecycle Security and Documentation

- **Secure OTA Updates:** Deliver firmware and software updates securely
- **Technical Documentation:** Maintain detailed specifications, risk assessments, and compliance evidence for EN 18031
- **CE Marking:** Signal adherence to RED-DA by marking all compliant products with the CE mark

5. Proactive Measures

- **Security by Design:** Integrate certified modules and secure coding practices during the design phase
- **Testing and Validation:** Perform internal and third-party penetration testing for EN 18031 compliance
- **Customer Support:** Provide integration guidance to customers for system-level compliance
- **Notifications:** Provide a form to sign-up for cybersecurity notifications at https://multitech.com/security/

MultiTech's Cybersecurity Framework

MultiTech follows the NIST Cybersecurity Framework (CSF), applying best practices for IoT device security. MultiTech evaluates its systems and processes against NISTIR standards to ensure integrity and resilience.

Core Capabilities:

- 24/7 Managed Detection and Response (MDR)
- Continuous vulnerability scanning
- Cybersecurity insurance with enforced 2FA
- Security Awareness Training (SAT) for all employees

Compliance Standards:

- SOC 2 – Customer data protection
- ISO 27001 – Information security roadmap

Manufacturing Security:

- Air-gapped networks isolated from enterprise systems
- Dedicated Cybersecurity Incident Response Team (CSIRT)

International and Regional Standards

MultiTech's CSIRT monitors and aligns with international and regional cybersecurity agencies and standards:

- NIST (US)
- MITRE CVE database
- Cyber Resilience Act (EU)
- PTSI (UK)
- California AB 1906 (US)
- ANATEL ACT 77 (Brazil)

Cybersecurity Incident Response Process (CSIRP)

1. Discovery

- Perform penetration testing by MultiTech, third parties, and customers
- Post public vulnerability announcements

2. Triage

- Complete severity and impact analysis
- Set action plans

3. Advisory

- Publish security advisories at https://multitech.com/security/

4. Remediation

- Provide software updates
- Communicate via product change notifications (PCNs) and release notes

Contact and Support

Questions?

Reach out to your MultiTech sales representative or explore our technical resources:

Security Advisories - Review industry news and announcements about device and software security issues

Support Portal - Create an account and submit a support case

MultiTech Website – Visit MultiTech's website for product news and information

World Headquarters – USA

+1 (763) 785-3500 | sales@multitech.com

EMEA – UK

+(44) 118 959 7774 | sales@multitech.co.uk