TDC NET

TECHNICAL OPERATIONS MANUAL

Document ID: SOP-005
Title: Network Security Incident Response
Category: Security
Equipment Types: Firewalls, Routers, Switches, Monitoring Systems
Applicable Fault Codes: SEC-001, SEC-002, SEC-003
Last Updated: 2025-10-04

NETWORK SECURITY INCIDENT RESPONSE

SECURITY THREAT IDENTIFICATION:

1. Monitor security alerts and anomalies
2. Analyze traffic patterns for suspicious activity
3. Review access logs for unauthorized attempts
4. Coordinate with cybersecurity team

IMMEDIATE CONTAINMENT:

1. Isolate affected network segments
2. Block suspicious IP addresses
3. Disable compromised user accounts
4. Activate additional monitoring

INVESTIGATION PROCEDURES:

1. Preserve evidence for forensic analysis
2. Document all security events
3. Identify attack vectors and methods
4. Assess potential data exposure

RECOVERY ACTIONS:

1. Restore services from clean backups

2. Apply security patches and updates

3. Reset compromised credentials

4. Implement additional security controls

REPORTING REQUIREMENTS:

1. Notify regulatory authorities if required

2. Inform affected customers

3. Document lessons learned

4. Update security procedures
