Durand Porter This document was created and completed in its entirety by Durand Porter

DURAND PORTER

STRATEGY. INNOVATION. IMPACT.

CYBERSECURITY COMPLIANCE & INCIDENT RESPONSE OPERATIONS MANUAL

Secure Operational Governance, Threat Response, and Regulatory Compliance Framework

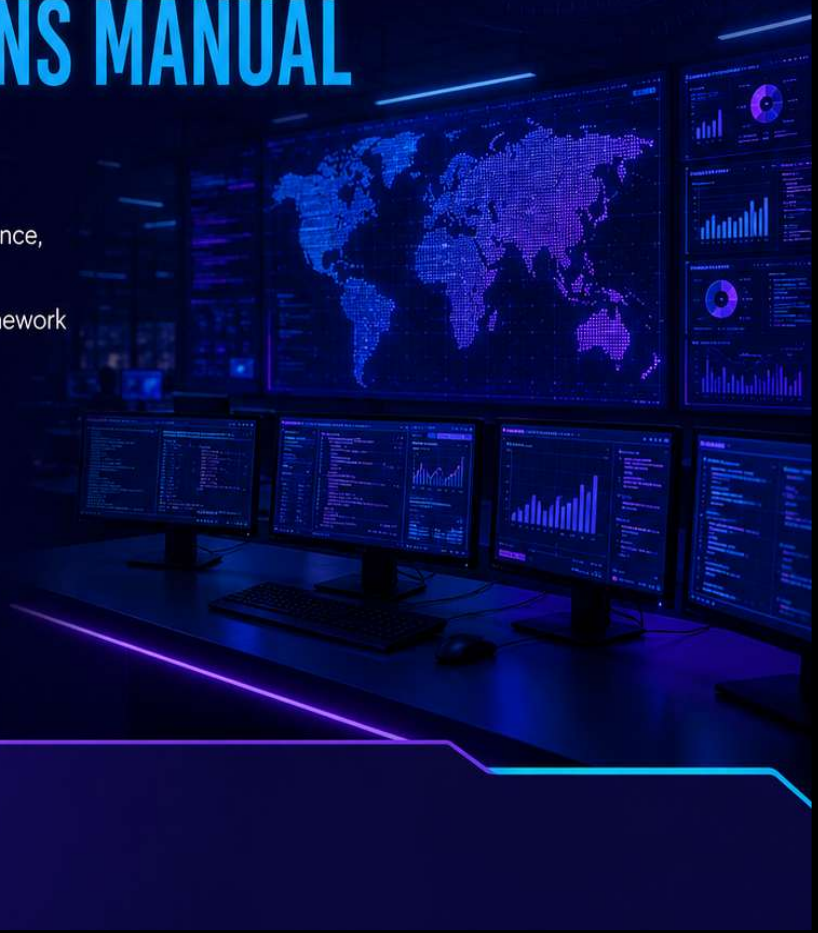

Table of Contents

1. Executive Summary

This manual establishes enterprise cybersecurity governance, operational security standards, compliance controls, and incident response procedures required to protect organizational infrastructure, applications, cloud services, operational technology systems, and sensitive data assets.

This manual provides standardized operational guidance for:

- Security Operations Center (SOC) management
- Continuous security monitoring
- Threat detection and escalation
- Incident response coordination
- Vulnerability remediation
- Regulatory compliance management
- Business continuity operations
- Disaster recovery planning
- Digital forensics and evidence preservation

All cybersecurity operations shall align with NIST Cybersecurity Framework (CSF), ISO/IEC 27001, CIS Controls, SOC 2, HIPAA, GDPR, and PCI-DSS compliance standards.

2. Governance & Compliance Framework

The organization shall maintain a formal cybersecurity governance structure to support enterprise-wide operational oversight, policy enforcement, risk management, and regulatory compliance activities.

The Cybersecurity Steering Committee is responsible for:

- Enterprise security governance
- Policy approval and review
- Cybersecurity budget oversight
- Risk management direction
- Executive-level reporting

The Chief Information Security Officer (CISO) maintains overall accountability for cybersecurity operations, compliance readiness, and incident escalation management.

Compliance reviews shall occur quarterly and include:

- Policy validation
- Access control audits
- SIEM log review
- Regulatory gap analysis
- Third-party risk assessments

3. Security Operations Center Procedures

The Security Operations Center (SOC) shall operate continuously to monitor enterprise infrastructure, identify suspicious activity, and coordinate incident response operations.

SOC Tier Structure:

Tier 1 - Security alert monitoring and triage

Tier 2 - Incident investigation and correlation

Tier 3 - Advanced threat analysis and containment

SOC analysts shall monitor:

- Authentication events
- Privileged account activity
- Malware detections
- Endpoint alerts
- Data transfer anomalies
- Cloud security events
- Network intrusion attempts

Critical incidents shall be escalated to the Incident Response Manager within fifteen (15) minutes of detection.

4. Incident Response Operations

The organization shall maintain a formal incident response lifecycle consisting of:

1. Preparation
2. Identification
3. Containment
4. Eradication
5. Recovery
6. Lessons Learned

Containment procedures may include:

- Isolation of compromised endpoints
- Suspension of privileged accounts
- Blocking malicious IP addresses
- Segmentation of affected networks
- Preservation of forensic evidence

Recovery activities shall validate system integrity prior to restoring production operations.

All incident investigations must maintain documented chain-of-custody procedures for forensic evidence handling.

5. Vulnerability Management Procedures

The vulnerability management program shall include:

- Automated vulnerability scanning
- Risk prioritization
- Patch validation
- Remediation tracking
- Compliance reporting

Scanning Frequency:

- Internet-facing systems - Weekly
- Internal infrastructure - Monthly
- Cloud environments - Continuous
- Critical infrastructure - Daily monitoring

Patch Remediation Standards:

Critical - 24 Hours

High - 72 Hours

Medium - 14 Days

Low - 30 Days

Unpatched critical vulnerabilities require executive escalation.

6. Identity & Access Management

The organization shall enforce strict identity and access management controls to prevent unauthorized access to enterprise systems and data assets.

Required controls include:

- Multi-factor authentication (MFA)
- Role-based access control (RBAC)
- Least privilege enforcement
- Privileged access monitoring
- Password complexity requirements
- Quarterly access reviews

Privileged accounts shall require:

- Formal approval
- Security monitoring
- Session logging
- Periodic review and recertification

Access violations shall trigger immediate SOC investigation procedures.

7. Network & Endpoint Security Standards

The network security architecture shall implement:

- Firewalls
- IDS/IPS technologies
- Secure VPN access
- Network segmentation
- Encrypted communications
- Continuous traffic inspection

Endpoint protection requirements include:

- Endpoint Detection & Response (EDR)
- Anti-malware protection
- Device encryption
- USB restriction policies
- Secure configuration baselines

Firewall rule reviews shall occur quarterly and follow deny-by-default security standards.

8. Threat Intelligence & Monitoring

Threat intelligence operations shall support proactive defense capabilities through continuous monitoring of emerging cybersecurity threats and adversary activity.

Threat intelligence sources include:

- Government advisories
- Commercial intelligence feeds
- Internal incident reports
- ISAC intelligence sources

Threat intelligence activities include:

- Indicator correlation
- Threat hunting
- Adversary analysis
- Detection rule development
- Malware analysis support

The SIEM platform shall aggregate enterprise security logs and generate automated alert escalation workflows.

9. Business Continuity & Disaster Recovery

The organization shall maintain documented disaster recovery and business continuity procedures to support operational resilience during disruptive cybersecurity events.

Recovery Objectives:

Recovery Time Objective (RTO): 4 Hours

Recovery Point Objective (RPO): 1 Hour

Disaster recovery procedures include:

- Secure backup validation
- Recovery testing
- Infrastructure failover procedures
- Restoration integrity checks
- Emergency communications

Disaster recovery exercises shall occur semi-annually and following major infrastructure modifications.

10. Audit & Compliance Procedures

Internal audit reviews shall validate:

- Security policy compliance
- Access control enforcement
- Incident response readiness
- Vulnerability remediation tracking
- Backup validation procedures
- Logging and monitoring controls

External assessments may include:

- Penetration testing
- Red team exercises
- Regulatory audits
- Third-party security reviews

Audit findings shall be documented, tracked, and remediated according to established compliance timelines.

11. Operational Appendices

Appendices shall include:

- Incident Severity Matrix
- Incident Response Checklist
- Escalation Matrix
- Evidence Chain-of-Custody Form
- Disaster Recovery Validation Checklist
- Compliance Mapping Matrix
- Security Audit Checklist
- Ransomware Response Procedures

Appendix A - Incident Severity Matrix

Severity	Impact	Response Time	Escalation
Critical	Enterprise-wide compromise	Immediate	Executive Leadership
High	Major operational disruption	< 1 Hour	CISO
Medium	Limited operational impact	< 4 Hours	SOC Manager
Low	Minor operational impact	< 24 Hours	Operations Team


DURAND PORTER
STRATEGY. INNOVATION. IMPACT.
THANK YOU
We appreciate the opportunity to partner on this critical mission. Together, we can drive innovation, enhance system capabilities, and build a more resilient future for aerospace.
Salt Lake City, UT, US, 84107
durandmporter@gmail.com
+1 8056378355