Incident Response Policy

Organization: AegisCISO
Document ID: POL-IR-001
Version: 1.0
Effective Date: January 2026
Classification: Internal
Owner: Chief Information Security Officer (CISO)

---

1. Purpose

This policy establishes the framework for detecting, responding to, and recovering from cybersecurity incidents to minimize impact on AegisCISO operations and protect information assets.

2. Scope

This policy applies to:

- All cybersecurity incidents affecting AegisCISO
- All employees, contractors, and third parties
- All information systems and data
- All locations and facilities

3. Incident Classification

3.1 Incident Categories

POL-IR-001-01: Incidents shall be classified by type.

Category	Description	Examples
Malware	Malicious software infection	Ransomware, virus, trojan, spyware
Unauthorized Access	Unauthorized system/data access	Account compromise, privilege escalation
Data Breach	Unauthorized data disclosure	Data exfiltration, accidental exposure
Denial of Service	Service availability impact	DDoS, resource exhaustion
Insider Threat	Malicious/negligent insider activity	Data theft, sabotage
Social Engineering	Manipulation attacks	Phishing, vishing, pretexting
Physical	Physical security breach	Unauthorized facility access, theft

3.2 Incident Severity

POL-IR-001-02: Incidents shall be assigned severity levels.

Severity	Description	Impact	Response Time
Critical (P1)	Major breach, business-critical sy	Significant financial/operational/re	Immediate (< 1 hour)
High (P2)	Significant breach, important syst	Notable impact to operations	< 4 hours
Medium (P3)	Limited breach, non-critical syste	Moderate impact, contained	< 24 hours

Low (P4)	Minor incident, minimal impact	Limited impact, easily resolved	< 72 hours

4. Incident Response Team

4.1 CSIRT Structure

POL-IR-001-03: Computer Security Incident Response Team (CSIRT) shall be established.

Core Team Members:

- Incident Response Manager (Lead)
- Security Analysts
- IT Operations Representative
- Network Engineer
- Legal Representative (as needed)
- Communications Representative (as needed)

4.2 CSIRT Responsibilities

POL-IR-001-04: CSIRT roles and responsibilities.

Role	Responsibilities
IR Manager	Overall incident coordination, escalation dec
Security Analyst	Technical investigation, evidence collection,
IT Operations	System isolation, recovery, service restorati
Network Engineer	Network forensics, traffic analysis, containm
Legal	Legal obligations, regulatory notifications,
Communications	Internal/external communications, media handl

4.3 Contact Information

POL-IR-001-05: Incident response contact list shall be maintained.

Requirements:

- 24/7 contact numbers for CSIRT members
- Backup contacts identified
- Escalation paths documented
- External contacts (law enforcement, regulators, vendors)
- Contact list reviewed quarterly

5. Incident Response Phases

5.1 Preparation

POL-IR-001-06: Preparation activities.

Requirements:

- Incident response plan documented and approved

- CSIRT trained and equipped
- Detection tools deployed
- Forensic capabilities available
- Communication templates prepared
- Regular tabletop exercises conducted

5.2 Detection and Analysis

POL-IR-001-07: Incident detection and analysis.

Detection Sources:

- Security monitoring tools (SIEM, EDR, IDS)
- User reports
- Third-party notifications
- Vendor alerts
- Threat intelligence
- Audit findings

Analysis Requirements:

- Initial triage within response time SLA
- Scope determination
- Impact assessment
- Evidence preservation
- Documentation of findings

5.3 Containment

POL-IR-001-08: Incident containment procedures.

Short-term Containment:

- Isolate affected systems
- Block malicious traffic
- Disable compromised accounts
- Preserve evidence
- Limit damage spread

Long-term Containment:

- Implement temporary fixes
- Apply additional monitoring
- Prepare for eradication
- Maintain business operations

5.4 Eradication

POL-IR-001-09: Threat eradication requirements.

Requirements:

- Remove malware and artifacts
- Patch vulnerabilities exploited

- Reset compromised credentials
- Clean or rebuild affected systems
- Verify complete removal

5.5 Recovery

POL-IR-001-10: System recovery procedures.

Requirements:

- Restore systems from clean backups
- Implement security improvements
- Gradual service restoration
- Enhanced monitoring during recovery
- User notification as appropriate

5.6 Post-Incident Activity

POL-IR-001-11: Post-incident review requirements.

Requirements:

- Incident report within 5 business days
- Lessons learned meeting
- Root cause analysis
- Improvement recommendations
- Policy/procedure updates
- Training updates

6. Reporting Requirements

6.1 Internal Reporting

POL-IR-001-12: Internal incident reporting.

Severity	Report To	Timeframe
Critical	CISO, CIO, CEO, Board	Immediate, then hourly
High	CISO, CIO, Department Head	< 4 hours, then daily
Medium	CISO, System Owner	< 24 hours
Low	Security Team	< 72 hours

6.2 External Reporting

POL-IR-001-13: External notification requirements.

Stakeholder	Trigger	Timeframe
NCA (CERT)	Significant cybersecurity incident	Within 24 hours
Law Enforcement	Criminal activity suspected	As appropriate
Regulators	Regulatory breach	Per regulation

Affected Individuals	Personal data breach	Within 72 hours
Business Partners	Partner data affected	As contractually required
Cyber Insurance	Covered incident	Per policy terms

6.3 Incident Documentation

POL-IR-001-14: Incident documentation requirements.

Required Documentation:

- Incident ticket/tracking number
- Timeline of events
- Systems and data affected
- Actions taken
- Evidence collected
- Personnel involved
- Communications sent
- Costs incurred
- Lessons learned

7. Evidence Handling

7.1 Evidence Collection

POL-IR-001-15: Digital evidence collection.

Requirements:

- Chain of custody maintained
- Evidence integrity preserved (hashing)
- Forensically sound collection methods
- Documentation of collection process
- Secure evidence storage

7.2 Evidence Preservation

POL-IR-001-16: Evidence preservation requirements.

Requirements:

- Full disk images where required
- Memory capture for active incidents
- Log preservation
- Network traffic capture
- Retention per legal requirements
- Access restricted to authorized personnel

8. Communication Protocols

8.1 Internal Communications

POL-IR-001-17: Internal communication during incidents.

Requirements:

- Secure communication channels
- Need-to-know basis
- Regular status updates
- Escalation notifications
- Clear and factual messaging

8.2 External Communications

POL-IR-001-18: External communication during incidents.

Requirements:

- All external communications approved by Communications/Legal
- Consistent messaging
- Factual and timely information
- Media inquiries directed to designated spokesperson
- Customer notifications per legal requirements

9. Business Continuity Integration

9.1 BCP Activation

POL-IR-001-19: Business continuity activation criteria.

BCP Activation Triggers:

- Critical systems unavailable > 4 hours
- Data center evacuation required
- Multiple locations affected
- Extended recovery expected

9.2 Coordination

POL-IR-001-20: Incident response and BCP coordination.

Requirements:

- IR and BC teams coordinate response
- Joint command structure for major incidents
- Resource sharing
- Unified communications

10. Third-Party Coordination

10.1 External Support

POL-IR-001-21: External incident response support.

External Resources:

- Forensic investigators (retainer)
- Legal counsel (cyber-specialized)
- Public relations firm
- Cyber insurance claim support
- Law enforcement contacts

10.2 Vendor Incidents

POL-IR-001-22: Third-party incident management.

Requirements:

- Vendor incident notification requirements in contracts
- Vendor incident assessment procedures
- Coordination protocols
- Data protection verification

11. Metrics and Reporting

11.1 Incident Metrics

POL-IR-001-23: Incident metrics to track.

Metrics:

- Number of incidents by type/severity
- Mean time to detect (MTTD)
- Mean time to respond (MTTR)
- Mean time to contain (MTTC)
- Mean time to recover
- Financial impact
- Root cause categories

11.2 Reporting

POL-IR-001-24: Incident reporting requirements.

Report	Frequency	Audience
Incident summary	Monthly	Security Team
Trend analysis	Quarterly	CISO, Management
Annual incident report	Annually	Board, Executive
Post-incident report	Per incident	Relevant stakeholders

12. Training and Testing

12.1 CSIRT Training

POL-IR-001-25: Incident response training.

Requirements:

- Annual IR training for CSIRT members
- Technical certifications encouraged
- Threat-specific training as needed
- External training and conferences

12.2 Exercises

POL-IR-001-26: Incident response exercises.

Exercise Type	Frequency	Participants
Tabletop	Quarterly	CSIRT + Management
Technical drill	Bi-annually	CSIRT
Full simulation	Annually	Organization-wide

13. Compliance

13.1 Regulatory Requirements

This policy supports compliance with:

- NCA Essential Cybersecurity Controls (ECC-1: 2-12)
- ISO/IEC 27001:2022 - A.16 Information Security Incident Management
- GDPR (breach notification)
- PCI DSS - Requirement 12.10

14. Roles and Responsibilities

All Employees

- Report suspected incidents immediately
- Preserve evidence
- Cooperate with investigations
- Follow containment instructions

CSIRT

- Respond to incidents per this policy
- Maintain IR capabilities
- Conduct post-incident reviews
- Improve IR processes

Management

- Support IR activities
- Allocate resources
- Make escalation decisions
- Approve external communications

CISO

- Overall IR program ownership
- Regulatory notifications
- Board reporting
- Resource allocation

15. Enforcement

Failure to report incidents or cooperation may result in disciplinary action. Intentional interference with incident response may result in termination and legal action.

16. Review

This policy shall be reviewed annually and after significant incidents.

17. References

- NCA Essential Cybersecurity Controls
- NIST SP 800-61 (Incident Handling)
- ISO/IEC 27035 (Incident Management)
- SANS Incident Response Process

Document Control:

Version	Date	Author	Changes
1.0	January 2026	CISO	Initial Release