Human Resources Cybersecurity Policy

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

---

1. Purpose

This policy establishes cybersecurity requirements for human resources processes throughout the employee lifecycle to protect AegisCISO information assets and ensure personnel security.

2. Scope

This policy applies to:

- All employees (permanent, temporary, part-time)
- All contractors, consultants, and third-party personnel
- All candidates and applicants
- Human Resources and hiring managers

3. Pre-Employment Security

3.1 Background Verification

POL-HR-001-01: Background verification shall be conducted for all personnel before granting access to AegisCISO systems and facilities.

Requirements:

- Criminal record check
- Employment history verification (minimum 5 years)
- Education credential verification
- Reference checks (minimum 2 professional references)
- Credit check for financial positions
- Security clearance verification where applicable

3.2 Job Descriptions

POL-HR-001-02: All job descriptions shall include cybersecurity responsibilities.

Requirements:

- Information security responsibilities clearly stated
- Required security certifications identified
- Authority levels and access requirements defined

- Reporting relationships documented

3.3 Terms and Conditions of Employment

POL-HR-001-03: Employment contracts shall include cybersecurity terms.

Requirements:

- Confidentiality and non-disclosure agreements
- Acceptable use policy acknowledgment
- Intellectual property agreements
- Post-employment obligations

4. During Employment

4.1 Management Responsibilities

POL-HR-001-04: Management shall ensure employee compliance with security policies.

Requirements:

- Communicate security policies to all staff
- Ensure appropriate access levels assigned
- Monitor for policy compliance
- Report security concerns promptly
- Lead by example in security practices

4.2 Security Awareness and Training

POL-HR-001-05: All personnel shall complete mandatory cybersecurity training.

Requirements:

Initial Training (within 30 days of start):

- Security awareness fundamentals
- Acceptable use policy
- Incident reporting procedures
- Phishing awareness
- Password security
- Physical security

Annual Refresher Training:

- Updated threat landscape
- Policy changes
- Incident lessons learned
- Role-specific security training

Specialized Training (role-based):

- Privileged user security
- Developer security (secure coding)
- Administrator security
- Executive cyber risk awareness

4.3 Disciplinary Process

POL-HR-001-06: A formal disciplinary process shall address security violations.

Violation Categories:

- Minor: First-time accidental violations (verbal warning, additional training)
- Moderate: Repeated minor violations or negligent behavior (written warning)
- Major: Intentional violations or gross negligence (suspension, termination)
- Critical: Malicious actions or data breach (immediate termination, legal action)

4.4 Performance Evaluation

POL-HR-001-07: Security compliance shall be included in performance evaluations.

Requirements:

- Security awareness training completion
- Adherence to security policies
- Incident reporting behavior
- Participation in security initiatives

5. Role Changes

5.1 Internal Transfers

POL-HR-001-08: Access rights shall be reviewed and adjusted upon role changes.

Requirements:

- Access review within 5 business days of transfer
- Removal of access no longer required
- Provision of new required access
- Updated training as needed
- Asset transfer documentation

5.2 Promotions

POL-HR-001-09: Privileged access shall be granted only after appropriate verification.

Requirements:

- Additional background check for elevated access
- Privileged access training completion
- Signed acknowledgment of responsibilities
- Manager approval documented

6. Termination and Exit

6.1 Voluntary Resignation

POL-HR-001-10: Secure offboarding shall be completed for departing employees.

Requirements:

- Exit interview including security debrief
- Knowledge transfer documentation
- Return of all assets (within final day)
- Access revocation (same day as departure)
- Reminder of ongoing confidentiality obligations

6.2 Involuntary Termination

POL-HR-001-11: Immediate access revocation for involuntary terminations.

Requirements:

- Access disabled before notification when feasible
- Physical access cards deactivated immediately
- Remote access disabled immediately
- Email forwarding configured (if appropriate)
- Asset recovery within 24 hours
- Security escort from premises if required

6.3 Contractor Termination

POL-HR-001-12: Contractor access shall be terminated upon contract end.

Requirements:

- Access expiration aligned with contract end date
- Access review 30 days before contract end
- Asset return verified before final payment
- NDA obligations confirmed

7. Access Provisioning

7.1 Access Request Process

POL-HR-001-13: Formal access request and approval process shall be followed.

Requirements:

- Business justification required
- Manager approval for standard access
- Data owner approval for sensitive data
- Security approval for privileged access
- Request retention for audit

7.2 Access Review

POL-HR-001-14: User access shall be reviewed quarterly.

Requirements:

- Manager certification of employee access
- Identification of dormant accounts
- Removal of unnecessary access

- Documentation of review results
- Exception approval and tracking

8. Special Categories

8.1 Privileged Users

POL-HR-001-15: Enhanced controls for privileged users.

Requirements:

- Enhanced background verification
- Specialized security training
- Activity monitoring and logging
- Periodic access recertification (monthly)
- Segregation of duties enforcement

8.2 Remote Workers

POL-HR-001-16: Security requirements for remote work arrangements.

Requirements:

- Remote work agreement signed
- Secure home office requirements documented
- VPN usage mandatory
- Approved device usage only
- Physical security of work materials

8.3 Temporary Staff

POL-HR-001-17: Limited access for temporary personnel.

Requirements:

- Access limited to specific duration
- Restricted to necessary systems only
- Enhanced monitoring during engagement
- Automatic access expiration configured

9. Training Records

9.1 Documentation

POL-HR-001-18: Training completion shall be documented and retained.

Requirements:

- Training completion certificates maintained
- Attendance records for awareness sessions
- Test scores for competency assessments
- Records retained for minimum 3 years

9.2 Metrics

Training metrics to be tracked:

- Training completion rates
- Average quiz scores
- Phishing simulation results
- Security incident correlation

10. Roles and Responsibilities

Human Resources

- Implement background verification processes
- Maintain training records
- Coordinate onboarding/offboarding
- Administer disciplinary process

IT Security

- Define security training requirements
- Develop training content
- Monitor compliance
- Manage access provisioning

Managers

- Ensure team compliance
- Approve access requests
- Conduct access reviews
- Report security concerns

Employees

- Complete required training
- Comply with policies
- Report incidents
- Return assets upon departure

11. Enforcement

Non-compliance with this policy will result in disciplinary action as defined in Section 4.3. HR and Security will jointly investigate policy violations.

12. Review

This policy shall be reviewed annually by HR and Security, with updates as needed for:

- Regulatory changes
- Organizational changes

- Incident lessons learned
- Industry best practices

13. References

- NCA Essential Cybersecurity Controls (ECC-1: 2-6)
- NCA Human Resources Cybersecurity Policy Template
- ISO/IEC 27001:2022 - A.6 Organization of Information Security

---

Document Control:

Version	Date	Author	Changes
1.0	January 2026	CISO	Initial Release