Example Security Policy

Version v2.1

PolicyPress

Last Reviewed: 2026-01-15

Contents

Purpose and Scope

PolicyPress recognizes that information is a critical asset that must be protected from threats, whether internal or external, deliberate or accidental. This Information Security Policy establishes the organization's commitment to protecting the confidentiality, integrity, and availability of all information assets.

Scope: This policy applies to all employees, contractors, vendors, and third parties who have access to PolicyPress's information systems and data.

Definitions

- **Information Asset**: Any data, system, network, or physical component that has value to the organization
- **Confidential Information**: Information that, if disclosed, could harm PolicyPress or its stakeholders
- **Security Incident**: Any event that compromises the security of information assets

Policy Statements

1. Access Control

All access to information systems must be authorized and based on the principle of least privilege. Users shall only be granted access necessary to perform their job functions.

Requirements

- Unique user identifiers for all system users

- Multi-factor authentication (MFA) for remote access and privileged accounts
- Regular access reviews conducted quarterly
- Immediate revocation of access upon termination or role change

2. Data Classification and Handling

PolicyPress classifies data into three categories:

Classification	Description	Examples	Handling Requirements
Public	Information intended for public disclosure	Marketing materials, public website content	Standard controls
Internal	Information for internal use only	Internal memos, policies	Access controls required
Confidential	Sensitive information requiring protection	[redacted]	Encryption required, strict access controls

3. Encryption Standards

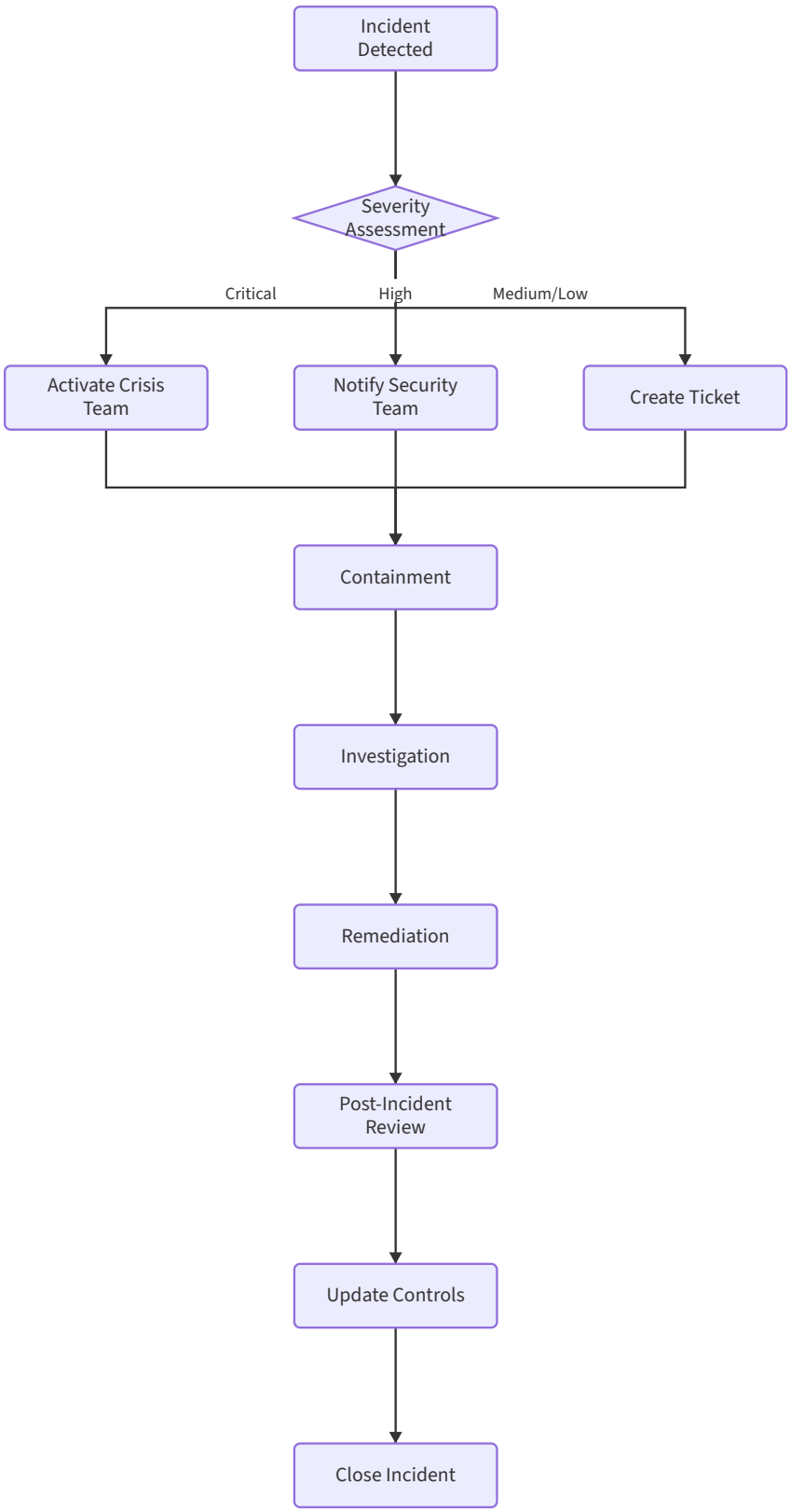
All sensitive data must be encrypted both at rest and in transit:

- **At Rest**: AES-256 encryption for stored data
- **In Transit**: TLS 1.3 or higher for network communications
- **Key Management**: Cryptographic keys must be stored in approved key management systems

Current encryption key rotation schedule: Every 90 days [redacted]

4. Incident Response Process

The following workflow illustrates our incident response process:


Incident Detected
Severity Assessment
Critical
High
Medium/Low
Activate Crisis Team
Notify Security Team
Create Ticket
Containment
Investigation
Remediation
Post-Incident Review
Update Controls
Close Incident

Response Time Objectives:

- Critical incidents: Response within 15 minutes
- High priority incidents: Response within 1 hour
- Medium priority incidents: Response within 4 hours
- Low priority incidents: Response within 24 hours

5. Security Awareness and Training

All personnel must complete security awareness training:

- Initial training upon hire
- Annual refresher training
- Role-specific training for IT and security staff
- Phishing simulation exercises quarterly

Roles and Responsibilities

Chief Information Security Officer (CISO)

- Overall accountability for information security program
- Reports security metrics to executive leadership
- Approves security policies and standards

Information Security Team

- Implements and maintains security controls
- Monitors security events and responds to incidents
- Conducts security assessments and audits

System Owners

- Responsible for security of their systems
- Ensure compliance with security policies
- Coordinate with security team on changes

All Personnel

- Follow security policies and procedures
- Report security incidents promptly
- Complete required security training
- Protect credentials and access tokens

> **NOTE** Annual compliance attestation is required from all staff with access to confidential data. Attestation records are retained for a minimum of three years.

> **TIP** Use the self-service compliance portal to complete your annual attestation - it takes less than five minutes and sends your manager an automatic confirmation.

> **WARNING** Access will be suspended automatically if the annual attestation is not completed within 30 days of the due date.

> **IMPORTANT: Legal Hold** If you receive a legal hold notice, do not delete or modify any documents, emails, or records without explicit written authorisation from Legal.

> **DANGER** Sharing credentials or bypassing MFA controls is a terminable offence and may trigger regulatory reporting obligations.

Compliance and Enforcement

Violations of this policy may result in disciplinary action, up to and including termination of employment or contract. PolicyPress reserves the right to pursue legal action for severe violations.

Monitoring and Auditing

Security controls and compliance are monitored through:

- Continuous security monitoring
- Quarterly access reviews
- Annual security audits
- Penetration testing (minimum annually)

Mathematical Risk Formula

The organization calculates risk using the following formula:

$$Risk = Threat \times Vulnerability \times Impact$$

Where:

- $Threat$ represents the likelihood of an attack (scale 1-5)
- $Vulnerability$ represents the exploitability (scale 1-5)
- $Impact$ represents potential damage (scale 1-5)

Risks scored above $R > 15$ require immediate mitigation.

Related Documentation

For more detailed information, please refer to:

- Acceptable Use Policy
- Incident Response Guide
- Security Awareness Training

Additional external resources:

- NIST Cybersecurity Framework
- ISO 27001 Information Security Standard

Code Examples

For automated compliance checking, security teams can use the following validation script:

```
def validate_password_strength(password):
    """
    Validates password meets minimum security requirements
    """
    requirements = {
```

```
        'length': len(password) >= 12,
        'uppercase': any(c.isupper() for c in password),
        'lowercase': any(c.islower() for c in password),
        'digit': any(c.isdigit() for c in password),
        'special': any(c in '!@#$%^&*()' for c in password)
    }
    return all(requirements.values()), requirements
```

Exception Process

Exceptions to this policy must be:

1. Documented with business justification
2. Approved by the CISO
3. Time-limited (maximum 90 days)
4. Reviewed at least monthly
5. Include compensating controls

Review and Updates

This policy shall be reviewed annually or whenever significant changes occur to:

- Business operations
- Regulatory requirements
- Threat landscape
- Technology infrastructure

Next scheduled review: January 15, 2027

Approval

This policy has been reviewed and approved by:

- John Doe, Chief Information Security Officer
- Jane Smith, Chief Technology Officer
- Board of Directors

For questions about this policy, contact security@example.com

Version History

Version	Date	Description	Revised By	Approved By
2.1	2026-01-15	Added cloud security requirements and updated incident response procedures.	Jane Smith	John Doe, CISO
2.0	2025-06-01	Updated encryption standards to align with NIST recommendations.	Jane Smith	John Doe, CISO
1.0	2024-01-15	Initial policy creation and approval.	Jane Smith	John Doe, CISO