Social Media Security Policy Template

Document Control Information

- **Document Title:** Social Media Security Policy
- **Document Version:** 1.0
- **Last Updated:** [DATE]
- **Document Owner:** [ROLE/NAME]
- **Approved By:** [ROLE/NAME]
- **Next Review Date:** [DATE]

1. Introduction

1.1 Purpose

This Social Media Security Policy establishes [ORGANIZATION NAME]’s requirements for the secure and appropriate use of social media platforms in accordance with ISO 27001:2022 requirements. It provides a framework for protecting organizational information, reputation, and security when using social media for business or personal purposes.

1.2 Scope

This policy applies to: - All employees, contractors, consultants, and third parties representing [ORGANIZATION NAME] - All social media platforms used for business or personal purposes that could affect the organization - All devices used to access social media, whether organization-owned or personal - All social media content that references or relates to the organization - All hours, whether during or outside of working hours

1.3 Policy Statement

[ORGANIZATION NAME] is committed to: - Enabling the effective use of social media for business purposes - Protecting organizational information when using social media - Maintaining the organization’s reputation on social media platforms - Preventing security incidents related to social media use - Ensuring compliance with legal and regulatory requirements - Providing guidance for appropriate social media behavior - Regularly reviewing and improving social media security controls

2. Business Use of Social Media

2.1 Authorized Business Accounts

- Official social media accounts shall be authorized and documented
- Authorization shall be provided by [ROLE/DEPARTMENT]
- Authorized accounts shall be registered in the social media inventory
- Account ownership shall be assigned to specific roles
- Account credentials shall be securely managed
- Account activity shall be regularly monitored
- Account security shall be regularly assessed
- Unauthorized accounts shall be reported and addressed

2.2 Account Management

- Social media account management shall be controlled
- Controls shall include:
  - Formal approval process for new accounts
  - Documented account ownership and responsibilities
  - Secure credential management
  - Multi-factor authentication where available
  - Regular access reviews
  - Prompt removal of access when no longer needed
- Account management procedures shall be documented
- Account management shall be regularly reviewed
- Account security incidents shall be promptly addressed

2.3 Content Guidelines

- Social media content shall follow established guidelines
- Guidelines shall include:
  - Brand and messaging standards
  - Information classification considerations
  - Approval requirements
  - Legal and regulatory compliance
  - Ethical standards
  - Crisis communication procedures
- Content guidelines shall be documented and communicated
- Content compliance shall be monitored
- Content guideline violations shall be addressed
- Content guidelines shall be regularly reviewed

2.4 Content Approval

- Social media content shall be approved before publication
- Approval requirements shall be based on content type and risk
- Approval shall be documented
- Approval procedures shall be established
- Emergency publication procedures shall be defined
- Approval compliance shall be monitored
- Approval procedures shall be regularly reviewed
- Approval exceptions shall be documented and justified

3. Personal Use of Social Media

3.1 Personal Use Guidelines

- Personal use of social media shall follow established guidelines
- Guidelines shall include:
  - Appropriate behavior when identifying as an employee
  - Protection of confidential information
  - Respect for intellectual property
  - Avoidance of conflicts of interest
  - Disclaimer requirements
  - Prohibited activities
- Guidelines shall be documented and communicated
- Guidelines shall be regularly reviewed
- Guideline violations shall be addressed
- Guidelines shall balance personal freedom with organizational protection

3.2 Disclaimer Requirements

- Employees identifying their employment shall use disclaimers
- Disclaimers shall clarify that views expressed are personal
- Disclaimer format shall be standardized
- Disclaimer requirements shall be documented and communicated
- Disclaimer compliance shall be monitored
- Disclaimer requirements shall be regularly reviewed
- Disclaimer exceptions shall be documented and justified

3.3 Prohibited Content

- Certain content shall be prohibited on personal social media
- Prohibited content shall include:
  - Confidential organizational information

    - Protected intellectual property
    - Defamatory or harassing content
    - Discriminatory content
    - False or misleading information about the organization
    - Content that violates laws or regulations
- Prohibited content shall be documented and communicated
- Prohibited content violations shall be addressed
- Prohibited content definitions shall be regularly reviewed

3.4 Working Hours Use

- Social media use during working hours shall be controlled
- Controls shall be appropriate to job role and requirements
- Controls may include:
    - Time limitations
    - Platform restrictions
    - Device restrictions
    - Network restrictions
- Controls shall be documented and communicated
- Control compliance shall be monitored
- Control violations shall be addressed
- Controls shall be regularly reviewed

4. Security Controls

4.1 Authentication Requirements

- Social media accounts shall use strong authentication
- Requirements shall include:
    - Strong passwords or passphrases
    - Multi-factor authentication where available
    - Unique credentials for each account
    - Regular credential rotation
    - Secure credential storage
- Authentication requirements shall be documented and communicated
- Authentication compliance shall be monitored
- Authentication failures shall be investigated
- Authentication requirements shall be regularly reviewed

4.2 Access Control

- Social media account access shall be controlled

- Controls shall include:
    - Role-based access
    - Principle of least privilege
    - Regular access reviews
    - Prompt removal of access when no longer needed
    - Monitoring of access attempts
- Access control procedures shall be documented
- Access control compliance shall be monitored
- Access control violations shall be addressed
- Access control shall be regularly reviewed

4.3 Device Security

- Devices used for social media shall be secured
- Security requirements shall include:
    - Current operating system and applications
    - Endpoint protection
    - Screen locking
    - Encryption where appropriate
    - Security configurations
- Device security shall be appropriate to device type and ownership
- Device security requirements shall be documented and communicated
- Device security compliance shall be monitored
- Device security incidents shall be addressed
- Device security shall be regularly reviewed

4.4 Network Security

- Networks used for social media shall be secured
- Security considerations shall include:
    - Avoidance of public unsecured networks
    - Use of VPN when appropriate
    - Network monitoring
    - Traffic filtering
- Network security requirements shall be documented and communicated
- Network security compliance shall be monitored
- Network security incidents shall be addressed
- Network security shall be regularly reviewed

5. Information Protection

5.1 Information Classification

- Information shared on social media shall be classified
- Classification shall follow the Data Classification Policy
- Classification shall determine sharing restrictions
- Classification shall be performed before sharing
- Classification shall be documented where appropriate
- Classification compliance shall be monitored
- Classification violations shall be addressed
- Classification guidance shall be provided to users

5.2 Confidential Information

- Confidential information shall not be shared on social media
- Confidential information shall be defined and communicated
- Procedures for identifying confidential information shall be established
- Accidental disclosure shall be promptly reported
- Disclosure incidents shall be managed according to the Incident Management Policy
- Confidential information protection shall be regularly assessed
- Confidential information handling shall be included in training
- Confidential information protection shall be regularly reviewed

5.3 Intellectual Property

- Intellectual property shall be protected on social media
- Protection shall include:
  - Copyright compliance
  - Trademark usage guidelines
  - Attribution requirements
  - Licensing considerations
- Intellectual property requirements shall be documented and communicated
- Intellectual property compliance shall be monitored
- Intellectual property violations shall be addressed
- Intellectual property protection shall be regularly reviewed

5.4 Personal Information

- Personal information shall be protected on social media
- Protection shall include:
  - Privacy compliance

    - Consent requirements
    - Data minimization
    - Retention limitations
- Personal information requirements shall be documented and communicated
- Personal information compliance shall be monitored
- Personal information incidents shall be addressed
- Personal information protection shall be regularly reviewed

6. Threat Management

6.1 Social Engineering Awareness

- Social media users shall be aware of social engineering threats
- Awareness shall include:
    - Phishing recognition
    - Impersonation detection
    - Suspicious link identification
    - Information gathering techniques
- Awareness training shall be provided
- Awareness materials shall be regularly updated
- Awareness effectiveness shall be assessed
- Awareness shall be reinforced through communications

6.2 Malware Protection

- Social media use shall include malware protection
- Protection shall include:
    - Link scanning
    - File scanning
    - Application security
    - Suspicious behavior recognition
- Protection requirements shall be documented and communicated
- Protection compliance shall be monitored
- Malware incidents shall be addressed
- Protection effectiveness shall be regularly assessed

6.3 Account Compromise

- Social media account compromise shall be addressed
- Procedures shall include:
    - Compromise detection
    - Reporting procedures
    - Containment actions

    - Recovery steps
    - Investigation process
- Procedures shall be documented and communicated
- Response effectiveness shall be regularly assessed
- Compromise incidents shall be analyzed for lessons learned
- Procedures shall be regularly reviewed and updated

6.4 Impersonation Management

- Social media impersonation shall be addressed
- Procedures shall include:
    - Impersonation detection
    - Reporting procedures
    - Platform notification
    - Legal actions when appropriate
    - Communication management
- Procedures shall be documented and communicated
- Response effectiveness shall be regularly assessed
- Impersonation incidents shall be analyzed for lessons learned
- Procedures shall be regularly reviewed and updated

7. Monitoring and Compliance

7.1 Social Media Monitoring

- Social media shall be monitored for security and compliance
- Monitoring shall include:
    - Brand mentions
    - Security threats
    - Policy compliance
    - Reputation issues
- Monitoring shall respect privacy requirements
- Monitoring shall be documented and communicated
- Monitoring findings shall be addressed
- Monitoring effectiveness shall be regularly assessed
- Monitoring shall be regularly reviewed

7.2 Incident Reporting

- Social media incidents shall be reported
- Reportable incidents shall include:
    - Account compromise
    - Information leakage

    - Policy violations
    - Reputation threats
    - Security breaches
- Reporting procedures shall be documented and communicated
- Reports shall be promptly investigated
- Reporting effectiveness shall be regularly assessed
- Reporting shall be included in security awareness training

7.3 Compliance Verification

- Social media compliance shall be regularly verified
- Verification may include:
    - Account reviews
    - Content audits
    - Security assessments
    - User interviews
- Verification shall be documented
- Non-compliance shall be addressed
- Verification effectiveness shall be regularly assessed
- Verification shall be regularly reviewed

7.4 Enforcement

- Social media policy violations shall be enforced
- Enforcement shall be:
    - Consistent
    - Fair
    - Proportional to the violation
    - Documented
- Enforcement procedures shall be established
- Enforcement shall follow HR procedures
- Enforcement shall be regularly reviewed
- Enforcement effectiveness shall be assessed

8. Training and Awareness

8.1 Social Media Training

- Social media users shall receive security training
- Training shall cover:
    - Policy requirements
    - Security best practices
    - Threat awareness

    - Incident reporting
    - Information protection
- Training shall be provided at onboarding and regularly thereafter
- Training completion shall be documented
- Training effectiveness shall be assessed
- Training materials shall be regularly updated

8.2 Security Awareness

- Social media security awareness shall be maintained
- Awareness activities may include:
    - Regular communications
    - Security alerts
    - Case studies
    - Best practices
    - Incident lessons learned
- Awareness shall address current threats
- Awareness effectiveness shall be assessed
- Awareness materials shall be regularly updated
- Awareness shall be integrated into organizational culture

8.3 Executive Guidance

- Executives shall receive specialized social media guidance
- Guidance shall address:
    - Heightened targeting risk
    - Reputation management
    - Strategic communications
    - Crisis management
    - Personal brand protection
- Guidance shall be personalized
- Guidance shall be regularly updated
- Guidance effectiveness shall be assessed
- Guidance shall be delivered by qualified personnel

9. Crisis Management

9.1 Social Media Crisis Identification

- Social media crises shall be promptly identified
- Identification criteria shall be established
- Criteria may include:
    - Volume of negative mentions

    - Influence of participants
    - Spread velocity
    - Content severity
    - Business impact
- Identification procedures shall be documented
- Identification effectiveness shall be regularly assessed
- Identification shall trigger appropriate response
- Identification criteria shall be regularly reviewed

9.2 Crisis Response

- Social media crises shall be effectively managed
- Management shall include:
    - Response team activation
    - Situation assessment
    - Communication strategy
    - Stakeholder management
    - Platform engagement
- Response procedures shall be documented
- Response shall be timely and appropriate
- Response effectiveness shall be assessed
- Response procedures shall be regularly reviewed
- Response shall be practiced through simulations

9.3 Recovery and Lessons Learned

- Social media crises shall be followed by recovery activities
- Activities shall include:
    - Reputation monitoring
    - Stakeholder communications
    - Policy and procedure review
    - Training updates
    - Preventive measures
- Lessons learned shall be documented
- Lessons shall be incorporated into procedures
- Recovery effectiveness shall be assessed
- Recovery procedures shall be regularly reviewed

10. Platform-Specific Security

10.1 Platform Risk Assessment

- Social media platforms shall be risk-assessed

- Assessment shall include:
  - Security features
  - Privacy controls
  - Data handling practices
  - Compliance capabilities
  - Known vulnerabilities
- Assessment shall be documented
- Assessment shall inform usage decisions
- Assessment shall be regularly updated
- Assessment shall consider emerging threats

10.2 Platform Security Features

- Platform security features shall be fully utilized
- Features may include:
  - Multi-factor authentication
  - Login alerts
  - Session management
  - Privacy controls
  - Content moderation
- Feature usage shall be documented
- Feature effectiveness shall be assessed
- Feature updates shall be monitored
- Feature usage shall be regularly reviewed

10.3 Platform-Specific Procedures

- Platform-specific security procedures shall be established
- Procedures shall address unique platform characteristics
- Procedures shall be documented and communicated
- Procedures shall be regularly updated
- Procedure compliance shall be monitored
- Procedure effectiveness shall be assessed
- Procedures shall be included in training

11. Roles and Responsibilities

11.1 Management

- Approve social media security policy
- Provide resources for social media security
- Review social media security performance
- Address significant social media security issues

- Support social media security initiatives
- Ensure compliance with requirements
- Approve risk acceptance when necessary

11.2 Information Security Team

- Develop and maintain social media security policy
- Define social media security requirements
- Review social media security controls
- Monitor social media security compliance
- Investigate social media security incidents
- Provide security guidance and expertise
- Report on social media security status

11.3 Marketing/Communications Team

- Manage official social media accounts
- Implement security controls for business accounts
- Create and approve official content
- Monitor brand presence on social media
- Respond to social media inquiries and issues
- Report security concerns to Information Security
- Support security awareness for social media

11.4 Human Resources

- Communicate social media policy to employees
- Address policy violations
- Support social media training
- Include social media requirements in onboarding
- Address social media issues affecting employees
- Support enforcement actions when necessary
- Provide guidance on personal use issues

11.5 All Users

- Comply with social media security policy
- Use social media securely and appropriately
- Protect organizational information
- Report security incidents and concerns
- Complete required training
- Follow security best practices
- Support security initiatives

12. Compliance and Exceptions

12.1 Compliance Monitoring

- Social media security compliance shall be regularly monitored
- Monitoring shall include:
  - Account security
  - Content compliance
  - User behavior
  - Security incidents
- Non-compliance shall be addressed
- Compliance trends shall be analyzed
- Compliance reports shall be provided to management
- Compliance monitoring shall be regularly reviewed

12.2 Exceptions

Exceptions to this policy shall be: - Documented with justification - Risk-assessed and approved by the Information Security Manager - Time-limited and regularly reviewed - Accompanied by compensating controls where appropriate - Tracked and reported - Minimized to the extent possible - Consistent with legal and regulatory requirements

13. Related Documents

- Information Security Policy
- Acceptable Use Policy
- Data Classification Policy
- Incident Management Policy
- Crisis Communication Plan
- Brand Guidelines
- [LIST OTHER RELEVANT POLICIES AND PROCEDURES]

14. Approval

This Social Media Security Policy is approved by:

Name: _____ Position: _____ Date: _____ Signature: _____