SANS Internet Policy Templates

XIONYC

Part I

General

Chapter 1

Acceptable Encryption Policy

Free Use Disclaimer

This policy was created by or for the SANS Institute for the Internet community. All or parts of this policy can be freely used for your organization. There is no prior approval required. If you would like to contribute a new policy or updated version of this policy, please send email to policy-resources@sans.org.

Things to Consider

Please consult the Things to Consider FAQ for additional guidelines and suggestions for personalizing the SANS policies for your organization.

Last Update Status

Updated June 2014

1.1 Overview

See 1.2.

1.2 Purpose

The purpose of this policy is to provide guidance that limits the use of encryption to those algorithms that have received substantial public review and

have been proven to work effectively. Additionally, this policy provides direction to ensure that Federal regulations are followed, and legal authority is granted for the dissemination and use of encryption technologies outside of the United States.

1.3 Scope

This policy applies to all COMPANY NAME employees and affiliates.

1.4 Policy

1.4.1 Algorithm Requirements

1. Ciphers in use must meet or exceed the set defined as "AES-compatible" or "partially AES-compatible" according to the IETF/IRTF Cipher Catalog, or the set defined for use in the United States National Institute of Standards and Technology (NIST) publication FIPS 140-2, or any superseding documents according to the date of implementation. The use of the Advanced Encryption Standard (AES) is strongly recommended for symmetric encryption.

2. Algorithms in use must meet the standards defined for use in NIST publication FIPS 140-2 or any superseding document, according to date of implementation. The use of the Rivest-Shamir-Adleman (RSA) and Elliptic Curve Cryptography (ECC) algorithms is strongly recommended for asymmetric encryption.

3. Signature Algorithms

Algorithms	Key Length (minimum)	Additional Comment
ECDSA	P-256	Cisco Legal recommends RFC 6090 compliance to avoid patent infringement.
RSA	2048	Must use a secure padding scheme. PKCS #7 padding scheme is recommended. Message hashing required.
LDWM	SHA256	Refer to LDWM Hash-based Signatures Draft.

1.4.2 Hash Function Requirements

In general, COMPANY NAME adheres to the NIST Policy on Hash Functions.

1.4.3 Key Agreement and Authentication

1. Key exchanges must use one of the following cryptographic protocols:
   - Diffie-Hellman,
   - Internet Key Exchange (IKE), or
   - Elliptic curve Diffie-Hellman (ECDH).
2. End points must be authenticated prior to the exchange or derivation of session keys.
3. Public keys used to establish trust must be authenticated prior to use. Examples of authentication include transmission via cryptographically signed message or manual verification of the public key hash.
4. All servers used for authentication (for example, Remote Authentication Dial In User Service (RADIUS) or Terminal Access Controller Access-Control System (TACACS)) must have installed a valid certificate signed by a known trusted provider.
5. All servers and applications using Secure Sockets Layer (SSL) or Transport Layer Security (TLS) must have the certificates signed by a known, trusted provider.

1.4.4 Key Generation

1. Cryptographic keys must be generated and stored in a secure manner that prevents loss, theft, or compromise.
2. Key generation must be seeded from an industry standard Random Number Generator (RNG). For examples, see NIST Annex C: Approved Random Number Generators for FIPS PUB 140-2.

1.5 Policy Compliance

1.5.1 Compliance Measurement

The Information Security (InfoSec) team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

1.5.2 Exceptions

Any exception to the policy must be approved by the InfoSec team in advance.

1.5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

1.6 Related Standards, Policies and Processes

- NIST Annex C: Approved Random Number Generators for FIPS PUB 140-2
- NIST Policy on Hash Functions

Part II

Application Security

Chapter 2

Web Application Security Policy

Free Use Disclaimer

This policy was created by or for the SANS Institute for the Internet community. All or parts of this policy can be freely used for your organization. There is no prior approval required. If you would like to contribute a new policy or updated version of this policy, please send email to policy-resources@sans.org.

Things to Consider

Please consult the Things to Consider FAQ for additional guidelines and suggestions for personalizing the SANS policies for your organization.

Last Update Status

Updated June 2014.

2.1 Overview

Web application vulnerabilities account for the largest portion of attack vectors outside of malware. It is crucial that any web application be assessed for vulnerabilities and any vulnerabilities by remediated prior to production deployment.

2.2 Purpose

The purpose of this policy is to define web application security assessments within COMPANY NAME. Web application assessments are performed to identify potential or realized weaknesses as a result of inadvertent mis-configuration, weak authentication, insufficient error handling, sensitive information leakage, etc. Discovery and subsequent mitigation of these issues will limit the attack surface of COMPANY NAME services available both internally and externally as well as satisfy compliance with any relevant policies in place.

2.3 Scope

This policy covers all web application security assessments requested by any individual, group or department for the purposes of maintaining the security posture, compliance, risk management, and change control of technologies in use at COMPANY NAME.

All web application security assessments will be performed by delegated security personnel either employed or contracted by COMPANY NAME. All findings are considered confidential and are to be distributed to persons on a "need to know" basis. Distribution of any findings outside of COMPANY NAME is strictly prohibited unless approved by the Chief Information Officer.

Any relationships within multi-tiered applications found during the scoping phase will be included in the assessment unless explicitly limited. Limitations and subsequent justification will be documented prior to the start of the assessment.

2.4 Policy

Web applications are subject to security assessments based on the following criteria:

1. New or Major Application Release New or Major Application Releases will be subject to a full assessment prior to approval of the change control documentation and/or release into the live environment.

2. Third Party or Acquired Web Application Third Party or Acquired Web Applications will be subject to full assessment after which it will be bound to policy requirements.

3. Point Releases Point Releases will be subject to an appropriate assessment level based on the risk of the changes in the application functionality and/or architecture.

4. Patch Releases Patch Releases will be subject to an appropriate assessment level based on the risk of the changes to the application functionality and/or architecture.

5. Emergency Releases An emergency release will be allowed to forgo security assessments and carry the assumed risk until such time that a proper assessment can be carried out. Emergency releases will be designated as such by the Chief Information Officer or an appropriate manager who has been delegated this authority.

All security issues that are discovered during assessments must be mitigated based upon the following risk levels. The Risk Levels are based on the Open Web Application Security Project (OWSAP) Risk Rating Methodology. Remediation validation testing will be required to validate fix and/or mitigation strategies for any discovered issues of Medium risk level or greater.

1. High Any high risk issue must be fixed immediately or other mitigation strategies must be put in place to limit exposure before deployment. Applications with high risk issues are subject to being taken off-line or denied release into the live environment.

2. Medium Medium risk issues should be reviewed to determine what is required to mitigate and scheduled accordingly. Applications with medium risk issues may be taken off-line or denied release into the live environment based on the number of issues and if multiple issues increase the risk to an unacceptable level. Issues should be fixed in a patch/point release unless other mitigation strategies will limit exposure.

3. Low Issue should be reviewed to determine what is required to correct the issue and scheduled accordingly.

The following security assessment levels shall be established by the InfoSec organization or other designated organization that will be performing the assessments.

1. Full A full assessment is comprised of tests for all known web application vulnerabilities using both automated and manual tools based on the OWSAP Testing Guide. A full assessment will use manual penetration testing techniques to validate discovered vulnerabilities to determine the overall risk of any and all discovered.
2. Quick A quick assessment will consist of a (typically) automated scan of an application for the OWSAP Top Ten web application security risks at a minimum.
3. Targeted A targeted assessment is performed to verify vulnerability remediation changes or new application functionality.

The current approved web application security assessment tools in use which will be used for testing are:

- Tool/Application 1
- Tool/Application 2
- Tool/Application 3

Other tools and/or techniques may be used depending upon what is found in the default assessment and the need to determine validity and risk are subject to the discretion of the Security Engineering team.

2.5 Policy Compliance

2.5.1 Compliance Measurement

The InfoSec team will verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

2.5.2 Exceptions

Any exception to the policy must be approved by the InfoSec team in advance.

2.5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. Web application assessments are a requirement of the change control process and are required to adhere to this policy unless found to be exempt. All application releases must pass through the change control process. Any web applications that do not adhere to this policy may be taken offline until such time that a formal assessment can be performed at the discretion of the Chief Information Officer.

2.6 Related Standards, Policies and Processes

- OWSAP Top Ten Project
- OWSAP Testing Guide
- OWSAP Risk Rating Methodology

2.7 Definitions and Terms

None.

2.8 Revision History

Date of Change	Responsible	Summary of Change
June 2014	SANS Policy Team	Updated and converted to new format.
2016-12-27	XIONYC	Conversion to LaTeX.