Root Zone KSK Operator Information Security Policy

Version 3.2

Root Zone KSK Operator Policy Management Authority

04 November 2020

Table of Contents

1 Introduction

Public Technical Identifiers (PTI) performs the Root Zone Key Signing Key (RZ KSK) Operator role pursuant to a contract from the Internet Corporation for Assigned Names and Numbers (ICANN).

Information security for key processes and systems is essential to the performance of the RZ KSK Operator services. Part of the RZ KSK Operator's responsibility is to manage, protect, and control these information assets to ensure the integrity of the RZ KSK Operator function. The RZ KSK Operator is committed to preserving the integrity, availability, and accountability of all physical and electronic information assets related to the RZ KSK Operator function.

This document is a capstone to the policy documents depicted in Appendix B.

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 (https://www.ietf.org/rfc/rfc2119.txt).

2 Objective and Scope

The objective of this policy is to ensure the establishment of preventive controls and measures for the identification, management, and monitoring of threats (whether internal or external, deliberate or accidental) to the information assets related to RZ KSK Operator function. The establishment and maintenance of an Information Security Management System (ISMS) will be used to manage the risk associated with information management and electronic operations of the RZ KSK Operator function.

This policy is applicable to all staff involved in the RZ KSK Operator function. This staff MUST comply with the policies found in this and other related information security documents. Staff who deliberately violate this or other information security policy statements will be subject to disciplinary action (which MAY ultimately include termination).

3 Roles and Responsibilities

The RZ KSK Operator has established four roles in information security, at least one of which applies to each staff member: Information Owner, Custodian, User, and RZ KSK Operations Security (RKOS). These roles define general responsibilities with respect to information security.

3.1 Information Owners

Each type of information MUST have an Owner. When information owners are not clearly implied by organizational design, the Root Zone KSK Operator Policy Management Authority (PMA) MUST make the designation. Information Owners do not legally own the information. They are individuals who make decisions on behalf of the organization at a certain level or in a specific area.

Information owners MUST designate a backup person to act if they are absent or unavailable. Owners MUST NOT delegate ownership responsibilities to third-party organizations, such as outsourcing organizations, or to any individual who is not a full-time employee. When both the owner and the backup owner are unavailable, immediate owner decisions MAY be made by the line manager who ordinarily handles the information.

3.2 Custodians

Custodians are in physical or logical possession of information and information systems. Like owners, custodians are specifically designated for different types of information. In many cases, a manager in the information systems department will act as the custodian. If a custodian is not clear, based on existing information system operational arrangements, then the PMA MUST designate a custodian.

Custodians MUST follow the instructions of owners and operate systems on behalf of owners, but also MUST serve users authorized by owners. Custodians MUST define the technical options, such as information criticality categories, and MUST permit owners to select the appropriate option for their information. Custodians also MUST define information system architectures and provide technical consulting assistance to owners, so information systems can be built and run that best meet business objectives. If requested, custodians MUST provide reports to owners about information system operations and information security problems.

Custodians MUST safeguard the information in their possession, including implementing access control systems to prevent inappropriate disclosure, and developing, documenting, and testing information system contingency plans.

3.3 Users

Users are not specifically designated but are broadly defined as any worker with access to internal information or internal information systems. They MUST follow all security requirements defined by owners and familiarize themselves with all information security requirements. They are also REQUIRED to participate in information security training and awareness efforts. Users MUST request access from their immediate manager and report all suspicious activity and security problems.

3.4 RZ KSK Operations Security

RKOS is the central point of contact, guidance, direction, and authority for all information security matters in relation to the RZ KSK Operations. Acting as internal technical consultants, it is the RKOS sole responsibility to create workable information security compromises that take into consideration the needs of users, custodians, owners, and selected third parties.

Reflecting these compromises, RKOS designs, establishes, and maintains information security standards, policies, guidelines, procedures, and other requirements applicable to the entire organization. RKOS MUST monitor the security of RZ KSK Operator information systems and provide information security training and awareness programs to staff as needed. RKOS MUST periodically provide management with reports about the current state of information security for the RZ KSK Operator function.

While contingency planning is the responsibility of custodians, the RKOS MUST provide technical consulting assistance related to emergency response procedures and disaster recovery. The RKOS also MUST organize an emergency response team to promptly respond to critical security emergencies for Root Domain Name System Security Extensions (DNSSEC) Key Management activities.

The RKOS is also responsible for ensuring that RZ KSK Operator functions are operating in a manner consistent with requirements and for investigating system intrusions and other information security incidents. Disciplinary matters resulting from violations of information security requirements are handled by managers working in conjunction with the Human Resources department.

4 Information Classification and Handling

4.1 Information Handling

Information that has been entrusted in relation to the RZ KSK Operator function MUST be protected in a manner commensurate with its sensitivity and criticality. Security measures MUST be employed regardless of the media on which information is stored, the systems that process it, or the methods by which it is moved. Information MUST be protected in a manner that is consistent with its classification, no matter what its stage in the lifecycle from origination to destruction.

4.2 Information Classification

The RZ KSK Operator has adopted an information classification scheme that categorizes information. All information under the RZ KSK Operator's control, whether generated internally or externally, falls into one of these categories: Secret, Confidential, Internal Use Only, or Public. All staff MUST familiarize themselves with the definitions for these categories and the steps to be taken to protect the information falling into each of these categories.

For purposes of this policy, "sensitive information" is information that falls into either the Secret or Confidential categories. The RZ KSK Operator's legal representation MAY also mark documents as 'Confidential and Privileged'.

4.3 Information Labeling

If information is sensitive, it MUST be labeled with an appropriate information classification designation from the time it is created until the time it is destroyed or declassified. Such markings MUST appear on all manifestations of the information.

The vast majority of the RZ KSK Operator information falls into the Internal Use Only category. For this reason, it is OPTIONAL to apply a label to Internal Use Only information. Information without a label is by default classified as Internal Use Only.

5 Information Access Control

5.1 Need to Know Concept

Access to information in the possession of or under the control of the RZ KSK Operator MUST be provided based on need to know. Information MAY be disclosed only to people who have a legitimate business need for the information. At the same time, staff MUST NOT withhold access to information when the owner of the information instructs that it be shared.

Staff MUST NOT attempt to access sensitive information unless the relevant owner has granted them access rights. When staff members change job duties, including termination, transfer, promotion, or leave of absence, their supervisor MUST immediately notify the RKOS. The privileges granted to all staff MUST be periodically reviewed by information owners and custodians to ensure that only those with a current need to know presently have access.

5.2 User IDs and Passwords

To implement the need-to-know process, each staff member accessing a multi-user information system MUST use a unique user ID and a private password. These user IDs MUST be employed to restrict system privileges based on job duties. Each staff member SHALL be personally responsible for the usage of his or her user ID and password.

5.3 Difficult-to-Guess Passwords/PINs

Users MUST choose passwords and PINs that are difficult to guess. This means that passwords MUST NOT be related to one's job or personal life. For example, a car license plate number, a spouse's name, birth date, or fragments of an address MUST NOT be used. This also means passwords MUST NOT be a word found in the dictionary or some other part of a speech or common phrase.

5.4 Third-Party Requests for RZ KSK Operator Information

Unless staff has been authorized by the information owner to make public disclosures, all external third-party requests for information about the RZ KSK Operator function MUST be referred to the RKOS. Such requests include questionnaires, surveys, and newspaper interviews.

RKOS will coordinate with the ICANN Communications team on an as needed basis.

5.5 External Disclosure of Security Information

Information about security measures for the RZ KSK Operator function is confidential and MUST NOT be released to people who are not authorized users of the involved systems unless approved by the PMA. For example, internal incident reports MAY be misinterpreted or be incomplete without proper review.

6 Physical Security

6.1 Physical Security to Control Information Access

Access to the Key Management Facility and other areas containing sensitive information MUST be physically restricted to those people with a need to know. When not in use, sensitive information MUST always be protected from unauthorized disclosure. During non-working hours, staff in areas containing sensitive information MUST lock up all information. Unless information is in active use by authorized people, desks MUST be clear and clean during non-working hours to prevent unauthorized access to information.

6.2 Theft Protection

All equipment MUST be physically secured with anti-theft devices if located in an open office. Servers and other multi-user systems MUST be placed in locked cabinets, locked closets, or locked rooms. Portable computers MUST be secured with locking cables, placed in locking cabinets, or secured by other locking systems when in an open office environment but not in active use.

7 Network Security

7.1 Internal Network Connections

All computers that store sensitive information and that are permanently or intermittently connected to internal computer networks MUST have a password-based access control system approved by the RKOS. Regardless of the network connections, all standalone computers handling sensitive information MUST also employ an approved password-based access control system.

7.2 External Network Connections

By default, all external connection capabilities MUST be disabled. Only external connections that have been expressly implemented to support the operation of the Key Management Facilities' systems MAY be enabled.

7.3 Network Changes

With the exception of emergency situations, all changes to networks MUST be documented and approved by RKOS. Changes to the RZ KSK Operator function networks MUST be made only by personnel who are authorized by RKOS. This process prevents unexpected changes from inadvertently leading to denial of service, unauthorized disclosure of information, and other problems. This process applies not only to staff but also to vendor personnel.

8 Formal Change Control

All hardware, software, and communications systems used for production processing MUST employ a documented change control process that is used to ensure that only authorized changes are made. This change control procedure MUST be used for all significant changes to production system software, hardware, communications links, and procedures.

9 Security Signoff

Before being used for production processing, new or substantially changed application systems MUST have received an approval from the RKOS for the controls to be employed.

10 Third-Party Compliance Audit

An annual Service Organization Control 3 (SOC 3) audit for the RZ KSK Operator function SHALL be performed by a public accounting firm, independent of PTI, ICANN, Verisign, and the auditor of Verisign. The auditor MUST be accredited by the American Institute of Certified Public Accountants (AICPA), who has demonstrated proficiency in the area and is widely recognized.

A copy of the RZ KSK Operator's Compliance Audit report and Management's Assertion in relation to SOC 3 compliance MUST be made available to the public.

With respect to compliance audits of the RZ KSK Operator's operations, significant exceptions or deficiencies identified during the Compliance Audit SHALL result in a determination of actions to be taken. The RZ KSK Operator's management MUST make such determinations with input from the auditor. The RZ KSK Operator's management MUST develop and implement corrective action plans. If the RZ KSK Operator determines that exceptions or deficiencies pose an immediate threat to the security or integrity of the RZ KSK, a corrective action plan MUST be developed within 30 days and

implemented within a commercially reasonable period of time. For less serious exceptions or deficiencies, the RZ KSK Operator's Management MUST evaluate the significance of such issues and determine the appropriate course of action.

11 Conduct Requirements

11.1 Prohibited Activities

Users MUST NOT test or attempt to compromise security measures unless specifically approved in advance by the PMA. Incidents involving unauthorized system penetration testing (e.g., system hacking, password guessing, file decryption, bootleg software copying, social engineering) or similar unauthorized attempts to compromise security measures MAY be unlawful and will be considered serious violations of the RZ KSK Operator's internal policy. Shortcuts bypassing system security measures, and misconduct (e.g., pranks and practical jokes) involving the compromise of system security measures are absolutely prohibited.

11.2 Unbecoming Conduct

The RZ KSK Operator's management reserves the right to revoke system privileges of any user at any time. Conduct that interferes with the normal and proper operation of information systems, which adversely affects the ability of others to use these information systems, or that is harmful or offensive to others is not permitted.

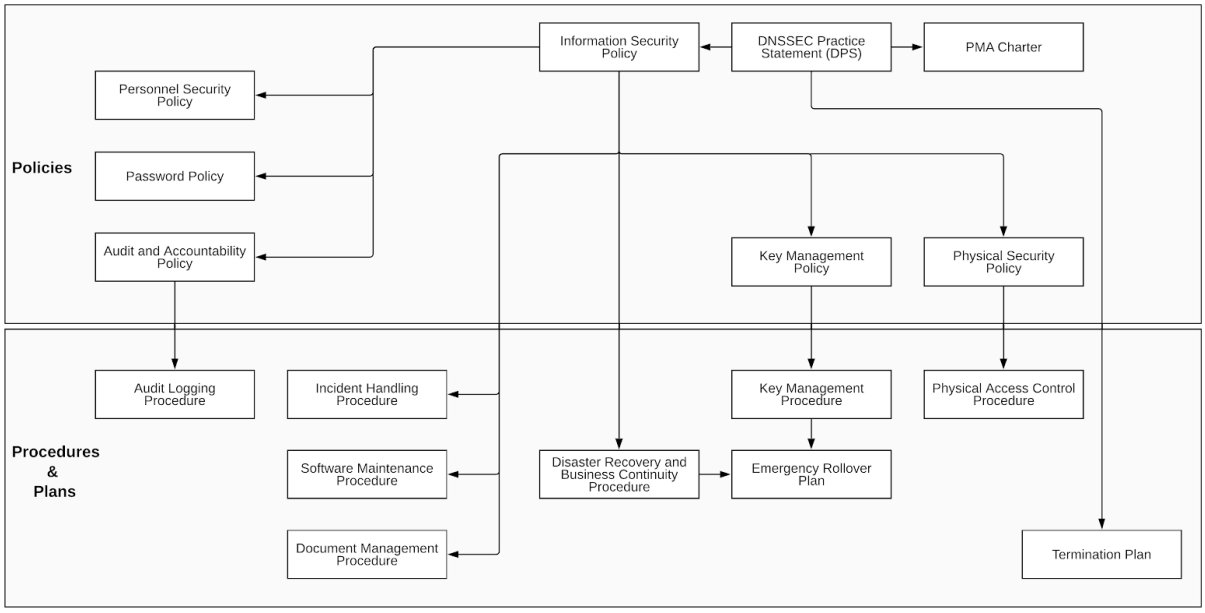
11.3 Mandatory Reporting

All suspected policy violations, system intrusions, malware infestations, and other conditions that might jeopardize the RZ KSK Operator function MUST be immediately reported to the RKOS. RKOS MUST assess the report and raise the issue to the PMA when appropriate.

Appendix A: Acronyms

AICPA	American Institute of Certified Public Accountants
DNSSEC	Domain Name System Security Extensions
ICANN	Internet Corporation for Assigned Names and Numbers
ISMS	Information Security Management System
KSK	Key Signing Key
PMA	Root Zone KSK Operator Policy Management Authority
PTI	Public Technical Identifiers
RFC	Request for Comments
RKOS	RZ KSK Operations Security
RZ	Root Zone
SOC	Service Organization Control

Appendix B: Structure of Supporting Information Security Documents



Appendix C: Change Log

Revision 3 - 04 October 2018

- Converted the document to use the latest Word template.
- Made minor editorial, formatting, and style changes.
- Made all cross-references hyperlinks.
- Adopted the RFC “MUST”, “SHOULD”, etc. convention throughout each document. Added a paragraph to Section 1 that explains the RFC wording convention.
- Added an acronym list.
- Cover: Changed the version from 2.3 to 3.0.
- Section 1: Wrote an introduction based on previous material from other parts of the document.
- Section 2: Added an Objective and Scope section. Clarified the document’s objective and scope.
- Section 3: Condensed text throughout the section to minimize redundancy.
- Section 4.2: Added Section 4.2.5 to define “reports” (moved text from Section 4.2.4).
- Section 4.4: Clarified how the document owner must differ from those in other roles.
- Section 6.2: Renamed the section to clarify the purpose and frequency of internal audits.

Revision 3.1 - 28 October 2019

- Annual review: Update version information and dates.
- Made minor editorial, formatting, and style changes.
- Updated section 5.4 to include ICANN Communications team.

Revision 3.2 - 04 November 2020

- Annual review: Update version information and dates.
- Appendix B: Diagram updated to reflect current PMA documents.