# Incident Management and Data Breach Policies & Procedures

## Introduction

Roots has procedures in place regarding the ongoing protection and monitoring of its digital assets. This document has been drafted to outline the policies and procedures which are used to respond to incidents involving data breaches or other information security incidents[1].

Roots's procedures are broken down into *phases*, which are outlined below, and are derived via globally accepted standards such as *ISO/IEC 27035*. The primary goal is to minimize the impact of such an incident as it pertains to clients, partners, employees, and Roots itself, as well as to continuously improve upon such procedures. The primary goals are to:

- Detect, report and assess information security incidents
- Respond to information security incidents, including the activation of appropriate controls to reduce, recover from, and prevent further impact

[1] ISO/IEC 27040 defines a data breach as: *a compromise of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to protected data transmitted, stored or otherwise processed*.

- Report information security vulnerabilities, so they can be assessed and dealt with appropriately
- Learn from information security incidents and vulnerabilities, institute additional preventive controls, and make improvements to the overall approach to information security incident management

# Roles and Responsibilities

A core team is designated to respond to incidents when they arise, and other teams within the organization are also provided responsibilities when the need arises to respond to a security incident. Those roles are outlined below:

| Role | Responsibilities | Trigger |
|---|---|---|
| CSIRT (Computer Security Incident Response Team) (Core Team) | • Act as "first-responders" to any reports of a new incident.<br>• Take all necessary steps to maintain and control integrity of all systems<br>• Report incidents to necessary personnel<br>• Maintain list of previous incidents | Any information security related events that occur |
| Legal | • Determine notification requirements<br>• Determine possible legal liabilities and duties | If the CSIRT determines the incident could require notification or privilege, or if legal action is a possibility |
| IT | • Provide IT related consultation to CSIRT<br>• Take appropriate internal steps to secure systems impacted by any | A security incident related to a system maintained by IT occurs |

| | | |
|---|---|---|
| | incident | |
| Communications | • Discuss, draft, and send written statements to affected parties, as well as stakeholders | When the CSIRT determines outside parties were affected, meaning communication is necessary |
| Data Protection Officer (DPO) | • Provide support to the CSIRT as needed<br>• File claims to insurance if necessary<br>• Be the POC for all internal inquiries regarding the incident | When any incident regarding data integrity occurs |

*Figure 1.1 Roles and Responsibilities*

# Response Process (Overview)

This response process is required following the detection/reporting of any security incident. The high-level steps are:

### Identification

Any and all collectable information is captured and shared with appropriate parties (such as the CSIRT, the DPO, IT).

### Analysis

The CSIRT analyzes the information and determines if a security incident has occurred. They will determine the severity of the incident, and provide information to the necessary parties.

### Containment

The CSIRT will contact relevant engineering/IT teams to further identify and address the issue.

### Eradication

The necessary teams identify the required steps to clean up the incident (i.e., apply patch, upgrade third-party library, deploy new software, notify customers, etc.) and track all tasks through to completion.

### Recovery

All affected systems are monitored once upgraded to ensure a smooth recovery, and to ensure that all identified vulnerabilities have been addressed.

### Reflection

A thorough review of the incident is conducted, including causes, steps to prevent, impact, resources required, etc. All findings are recorded and reviewed quarterly to ensure new systems have addresses all prior findings.

## Response Process (Detailed)

### Identification

**Detect**

Detection can result from many sources with a few examples being:

- Noticed internally via network logging, software logging, etc.
- Noticed externally via third party tool, such as AWS GuardDuty
- Reported by a client
- Reported by an employee
- Reported via White-Hat or Black-Hat individuals

All reports are taken seriously and should be analyzed immediately by the receiving team.

### Report

A detection that has been determined to have merit shall immediately be reported to the CSIRT.

## Analysis

### Verify

The CSIRT is responsible for verifying if the event occurred or is still occurring. Furthermore, they shall determine if Personally Identifiable Information (PII)[2] was, or reasonably believed to have been, acquired or accessed by an unauthorized person. To determine this, a few factors will be taken into consideration:

- A physical device (such as a computer, phone, tablet) is in the possession of an unauthorized individual, and such device contains or has access to personal information.
- Personal information has been downloaded or copied via unauthorized access to the information.
- Personal information has been used by an unauthorized source to log in to a system, open new accounts, etc.
- Personal information has been accessed by individuals without permission or without required authority.

### Incident Severities

| Level | Response Time | Description | Response |
|---|---|---|---|
| **SEV (Severity Level) 1** | **1 hour** | Events with significant security implications, which may directly impact the integrity of the environment. | *Ongoing* - A member of the CSIRT will monitor the case 24x7 until it is resolved. |

[2] In the ISO 27018 standard, ISO describes PII as "any information that (a) can be used to identify the PII principal to whom such information relates, or (b) is or might be directly or indirectly linked to a PII principal."

| | | | |
|---|---|---|---|
| | | Poses an immediate threat to certain data storages, credentials, etc.<br>(CAT 1, CAT 2, CAT 3) | *Resolution* - A member of CSIRT will work the case during normal working hours. |
| **SEV (Severity Level) 2** | **4 hours** | Malware or Malicious Code has been detected to be in production, or password changes/abuses have been detected. Multiple assets affected.<br>(CAT 1, CAT 2, CAT 3, CAT 7) | *Ongoing* - A member of the CSIRT will monitor the case 24x7 until it is resolved.<br>*Resolution* - A member of CSIRT will work the case during normal working hours. |
| **SEV (Severity Level) 3** | **1 Day** | Events affecting a few or a single asset(s), of which security context that may have grander implications. (CAT 2, CAT 3, CAT 4, CAT 7) | *Ongoing* - The case is handled with resources available.<br>*Resolution* - The case is handled with resources available. |
| **SEV (Severity Level) 4** | **2 Days** | SEV 4 is for policy/working violations, and events that have been flagged as having the possibility of grander security implications.<br>(CAT 4, CAT 5, CAT 6, CAT 7) | *Ongoing* - The case is handled with resources available.<br>*Resolution* - The case is handled with resources available. |

*Figure 1.2 Internal Severities*

| **Level** | **Description** |
|---|---|
| **CAT 1** | Unauthorized Access, Compromised machine, Compromised Asset, Data Theft, Espionage etc. |
| **CAT 2** | Denial of Service (DoS/DDoS) |
| **CAT 3** | Malware or Malicious Code |
| **CAT 4** | Reconnaissance or Scans or Probes etc. |
| **CAT 5** | Policy Violations or Improper Usage |

| | |
|---|---|
| **CAT 6** | Suspicious network activity / application behavior. |
| **CAT 7** | Other or Uncategorized |

*Figure 1.3 Categorization of Severity*

## Containment

The following will outline the steps for containing/handling all compromised systems/environments for the duration of the incident.

- Restrict all access to compromised machines
    - Do not log on to the machine
    - Do not change passwords on machine
    - Do not undergo any activity as an elevated privilege such as Root or Admin
- Isolate network connectivity of the compromised machine(s)
- Keep a detailed record of all activity
- Preserve all logs and electronic evidence
- Disable affected user accounts and change passwords

Identify and recover all electronic records or logs relevant to the time window of the incident and/or all affected machine(s). Store all recovered information on a secure device.

Ensure no one logs into any affected machines, unless granted explicit permission from the CSIRT.

## Eradication

After full containment of the incident, eradication procedures can begin. Eradication consists of the cleaning of all affected machines before returning to operations to ensure that the incident cannot be restarted, and all security keys, secrets, and tokens are rotated.

## Recovery

All necessary updates to prevent further incidents of similar type/origin must be applied in as short a time as possible. Systems must be patched/upgraded/updated as needed.

Any policies/procedures that could be improved to ensure quicker response to future incidents should be updated.

### Notification

Determine if notifications to clients or stakeholders are necessary. This decision is made by the CSIRT with Legal counsel as to what regulations are legally required. Notifications are encouraged, whether or not they are required by law.

### Germany

Germany has enacted the Federal Data Protection Act (BDSG) to protect the individual against their right to privacy being impaired through the handling of their personal data. Roots will abide by these laws, and will determine the legal requirement of a notification on a case-by-case basis.

### United States

Notification in the United States is governed by state and federal laws. Legal counsel will be consulted to determine the legal requirement of a notification on a case-by-case basis.

### Notification to Third Parties

Notification to government entities/law-enforcement will be assessed to determine if such notification would provide a benefit to either

- The recovery of lost data
- The uncovering of responsible parties

Such notification will be provided with all relevant evidence uncovered in previous steps.

## Reflection

The CSIRT will identify “Lessons Learned” in regards to this specific incident, and submit a report which will be viewable to all employees at Roots. Engineering/IT resources will be required to review this report, and identify possible steps to be taken within their scopes to prevent further incidents of a similar type. The information security organization, DPO, and the CSIRT will be responsible for elevating tasks that will lead to improved data security.

# Appendix

## Appendix A: German Federal Data Protection Act: Section 42a

### Section 42a Obligation to report unlawful access to data

If a private body as defined in Section 2 (4) or a public body as defined in Section 27 (1) first sentence No. 2 determines that

1. special types of personal data (Section 3 (9)),
2. personal data subject to professional secrecy,
3. personal data related to criminal offences or administrative offences or the suspicion of punishable actions or administrative offences, or
4. personal data concerning bank or credit card accounts

stored with that body have been unlawfully transferred or otherwise unlawfully revealed to third parties, with the threat of serious harm to the data subject's rights or legitimate interests, then in accordance with sentences 2 to 5 the body shall notify the responsible supervisory authority and the data subject without delay. The data subject shall be notified as soon as appropriate measures have been taken to protect the data and notification would no longer put criminal prosecution at risk. The notification for the data subjects shall describe the nature of the unlawful access and include recommendations for measures to minimize possible harm. The notification for the competent supervisory authority shall also describe possible harmful consequences of the unlawful access and measures taken by the body. Where notifying the data subjects would require unreasonable effort, in particular due to the large number of cases involved, such notification may be replaced by public advertisements of at least one-half page in at least two national daily newspapers, or by another equally effective measure for notifying the data subjects. A notification distributed by the body required to provide notification may be used

against that body in criminal proceedings or in proceedings in accordance with the Administrative Offences Act, or against an associate of the body required to provide notification as defined in Section 52 (1) of the Code of Criminal Procedure only with the consent of the body required to provide notification.

# Appendix B: EU General Data Protection Regulation (EU-GDPR) Article 33

## EU General Data Protection Regulation (EU-GDPR)

### Article 33 - Notification of a personal data breach to the supervisory authority

=> Article: 4

=> Recital: 75, 85, 87, 88

=> administrative fine: Art. 83 (4) lit a

1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

=> Recital: 75

2. The processor shall notify the controller without undue delay after becoming aware of a personal data breach.

3. The notification referred to in paragraph 1 shall at least:

(a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
(b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
(c) describe the likely consequences of the personal data breach;
(d) describe the measures taken or proposed to be taken by the controller to address the

personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

4. Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

5. The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken.

# Appendix C: EU General Data Protection Regulation (EU-GDPR) Article 34

## EU General Data Protection Regulation (EU-GDPR)

### Article 34 - Communication of a personal data breach to the data subject

=> Article: 4

=> Recital: 75, 86, 87, 88

=> administrative fine: Art. 83 (4) lit a Opening clause!

1. When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.

=> Recital: 75

2. The communication to the data subject referred to in paragraph 1 of this Article shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in points (b), (c) and (d) of Article 33(3).

3. The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met:

(a) the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;

(b) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise;

(c) it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

4. If the controller has not already communicated the personal data breach to the data subject,

the supervisory authority, having considered the likelihood of the personal data breach resulting in a high risk, may require it to do so or may decide that any of the conditions referred to in paragraph 3 are met.

# Appendix D

**Related Policies**

- Threat and Vulnerability Management Policies and Procedures
- GDPR Compliance Statement

**Functional Area**

- Information Security

**Process Owner**

- Douglas Franklin, DPO

**Reviewer**

- Kevin Corliss, CEO