Policies and Procedures

Cronitor Information Security Team

Purpose of this Document

This document acts as a table of contents for Cronitor Information Security policies and procedures. It links to separate documents. These documents are available internally for Cronitor team members, and may be shared via PDF with external parties at the discretion of the Cronitor Information Security Team.

Policies and Procedures

Implementation Information

Review Frequency	Annual
Responsible Person	Head of Information Security
Approved By	CEO
Approval Date	2021/11/10

Revision History

Version	Date	Description
1.0	2021/11/10	Initial document
1.1	2023/09/22	Specify policy period for Disaster Recovery testing

Disaster Recovery Procedure

Cronitor Information Security Team

Procedure Purpose

The purpose of this procedure is to ensure the continuity and recovery following the loss of IT Resources.

Procedure Statement

Wherever possible, Cronitor relies on cloud infrastructure (Amazon Web Services, Google Cloud, etc) with geographically distributed data storage. This enables us to use high-availability systems without building them ourselves.

For any systems that aren't built upon geo-redundant data backup, the department or team that owns the system must specify an independent disaster recovery plan to be reviewed by the Cronitor Information Security Team.

Disaster recovery procedures should be tested once per policy review period, with learnings incorporated into this procedure..

Implementation Information

Review Frequency	Annual
Responsible Person	Head of Information Security
Approved By	CEO
Approval Date	2021/11/09

Revision History

Version	Date	Description
1.0	2021/11/09	Initial document
1.1	2023/11/04	Add requirement for annual disaster recovery tests

Employee Deactivation Procedure

Cronitor Information Security Team

Procedure Purpose

To outline the steps that must be taken when the relationship is terminated or suspended with any worker (employee, contractor, etc) who had access to Cronitor software tools and data.

Procedure Statement

Immediate deactivation via Google Workspace. Worker’s supervisor may elect to create an alias for continuity of email.

Workers are deactivated via a checklist. The list is documented by IT for audit purposes to review individual deactivations. Revoke authentication for Cronitor applications, and for all other cloud services where possible. Include services identified below, plus any other services identified by the worker’s supervisor.

Immediate repossession of physical assets.

Services to Deactivate

Including, but not limited to:

- Cronitor website/admin tools
- Slack
- AWS
- Trello
- Sentry
- Drift
- Sendgrid
- Loops
- Zoom

Implementation Information

Review Frequency	Annual
Responsible Person	Head of Information Security
Approved By	CEO
Approval Date	2021/11/08

Revision History

Version	Date	Description
1.0	2021/11/08	Initial document
1.1	2023/09/25	Replace Mailchimp with Loops

Incident / Breach Response Procedure

Cronitor Information Security Team

Procedure Purpose

This Policy/Procedure specifies

- the responsibilities of all members of the Cronitor community when responding to or reporting information security incidents
- a method of reporting suspected theft, breach, or exposure of Cronitor data to the appropriate departments

Procedure Statement

- Any individual who suspects that a theft, breach, or exposure of data has occurred must immediately provide a description of what happened to the Head of Information Security via email sent to security@cronitor.io.
- The Information Security Team handles the incident response process, notifying and engaging external resources as needed and required by law. All communications with external law enforcement authorities are made after consulting with company counsel.
- The incident process encompasses six phases as defined in NIST SP 800--61
  - **Detection** is the discovery of the event with security tools or notification by an inside or outside party about a suspected incident. This phase includes the declaration and initial classification of the incident.
  - **Containment** is the triage phase where the affected host or system is identified, isolated or otherwise mitigated, and when affected parties are notified and investigative status established. This phase includes sub--procedures for seizure and evidence handling, escalation, and communication.
  - **Investigation** is the phase where ISO personnel determine the priority, scope, and root cause of the incident.
  - **Remediation** is the post--incident repair of affected systems, communication and instruction to affected parties, and analysis that confirms the threat has been contained. The determination of whether there are regulatory requirements for reporting the incident (and to which outside parties) will be made at this stage in cooperation with OGC. Apart from any formal reports, the post--mortem will be completed at this stage as it may impact the remediation and interpretation of the incident.
  - **Recovery** is the analysis of the incident for its procedural and policy implications, the gathering of metrics, and the incorporation of “lessons learned” into future response activities and training.

Implementation Information

Review Frequency	Annual
Responsible Person	Head of Information Security
Approved By	CEO
Approval Date	2021/11/09

Revision History

Version	Date	Description
1.0	2021/11/09	Initial document
1.1	2023/10/03	Update Head of Security email address

New Employee Training Procedure

Cronitor Information Security Team

Procedure Purpose

This Procedure specifies how new employees are acquainted with best practices in information security.

Procedure Statement

Within one month of their start date, all new employees with access to Cronitor software tools are required to take Information Security Training.

The training program involves a one hour time commitment to review slides/videos. The Infosec team maintains the curriculum and can provide it to existing employees upon request. The curriculum is branched from materials developed by TreeTop Security.

A participant is considered to have completed their training once they send a followup email to the infosec team citing two things they learned in the training, and two new habits they will develop as a result of the training.

Implementation Information

Review Frequency	Annual
Responsible Person	Head of Information Security
Approved By	CEO
Approval Date	2021/11/08

Revision History

Version	Date	Description
1.0	2021/11/08	Initial document
1.1	2023/09/24	Specify one month period for completion of Information Security Trainging

Vulnerability Management Procedure

Cronitor Information Security Team

Procedure Purpose

This Procedure specifies the rules for the review, evaluation, application, and verification of system updates to mitigate vulnerabilities in the IT environment and the risks associated with them.

Procedure Statement

Endpoint Protection (Anti-Virus & Malware)

- All owned and/or managed applications must use the Cronitor Infosec team-approved management approved endpoint protection software and configuration.
- All owned workstations and laptops must use Cronitor Infosec team-approved endpoint protection software and configuration, prior to any connection to any elevated-privilege accounts on applications.
- The endpoint protection software must not be altered, bypassed, or disabled.
- Each email gateway must utilize Cronitor Infosec team-approved email virus protection software and must adhere to our rules for the setup and use of this software, which includes, but is not limited to, scanning of all inbound and outbound emails.
- Controls to prevent or detect the use of known or suspected malicious websites must be implemented.
- All files received over networks or from any external storage device must be scanned for malware before use.
- Every virus that is not automatically cleaned by the virus protection software constitutes a security incident and must be reported to the Cronitor Infosec team.

Patch Management

- The Cronitor Infosec team maintains overall responsibility for patch management implementation, operations, and procedures.
- All owned and/or managed applications must be scanned on a regular basis to identify missing updates.
- All missing software updates must be evaluated according to the risk they pose to the organization.
- Missing software updates that pose an unacceptable risk to our applications must be implemented within a time period that is commensurate with the risk as determined by the Cronitor Infosec team.
- Software updates and configuration changes applied to applications must be tested prior to widespread implementation.

- Verification of successful software update deployment will be conducted within a reasonable time period.

Penetration Testing

- Penetration testing of the internal network, external network, and hosted applications must be conducted at least biennially or after any significant changes to the environment.
- Any exploitable vulnerabilities found during a penetration test will be corrected and re-tested to verify the vulnerability was corrected.

Implementation Information

Review Frequency	Annual
Responsible Person	Head of Information Security
Approved By	CEO
Approval Date	2021/11/10

Revision History

Version	Date	Description
1.0	2021/11/10	Initial document
1.1	2023/09/22	Specify policy period for Penetration Testing