SOC2 Policies for Initrobe

# **Security Architecture Narrative**

Initrobe contacted WARCSECURITYUNIT for a security review and recommendations. Initrobe is looking to expand operations and build new partnerships. In order to do so, introbe's security practices must be reviewed and changed. Furthermore, initrobe is looking to pursue a SOC2 Type 2 audit this year, its top priority is to create a security recommendation document.

Among other gaps, there are no formal incident response, business continuity and no recovery procedures. Introbe lacks a consolidated or centralized program for management and access or usage audit for ad-hoc assortment of additional vendors and tools (zoom,salesforce,shortcut,adobe,microsoft office) that some people have access and/or admin rights to.

The following outlines a series of recommendations to address the above mentioned issues and upgrade introbe’s current security posture outlining the first steps to pursue SOC2 Type 2 compliance.

# **Initrobe Product Architecture**

* AWS
* Azure
* Heroku
* GitHub

It’s crucial to define ownership for each cloud service

# **Initrobe Infrastructure**

## **Product Infrastructure**

Initrobe’s product infrastructure is cloud based. This means that robust authentication and authorization must be defined and implemented.

## **Authorized Personnel**

List the authorized people (CTO, System Admins, etc) within the system.

1. HRIS - 10 Employees
2. 80 Employees (expected to hire 30 more this year!)
3. 25 Contractors (1099)

## **IT Infrastructure**

Initrobe uses the following services for its internal infrastructure:

1. Google Cloud
2. AWS
3. Heroku
4. Slack
5. Slab
6. Shortcut

Access to these cloud services is limited according to the role of the employee and is reviewed quarterly as well as via regular onboarding/offboarding tasks for new and departing employees.

# **Initrobe Workstations**

Initrobe workstations are hardened against logical and physical attack by the following measures:

1. Encrypted hard drive
2. Automatic screen lock
3. Antivirus installed and scanning
4. Automatic OS updates enabled
5. Configured to use a password manager application

Workstation compliance with these measures is evaluated on a quarterly basis.

## **Remote Access**

Many Initrobe employees work remotely on a regular basis and connect to production and internal IT systems via the same methods as those employees connecting from the Initrobe physical office, i.e., direct encrypted access to cloud services. It is the employee’s responsibility to ensure that only authorized personnel use Initrobe resources and access Initrobe systems.

## **Access Review**

Access to Initrobe infrastructure, both internal and product, is reviewed quarterly and inactive users are removed. Any anomalies are reported to the security team for further investigation. When employees start or depart, an onboarding/offboarding procedure is followed to provision or deprovision appropriate account access.

## **Penetration Testing**

Initrobe commissions an external penetration test on a QUARTERLY basis. All findings are immediately reviewed and addressed to the satisfaction of the CTO/CEO.

# **Initrobe Physical Security**

Initrobe has one physical location, in the USA. Key issuance is tracked by the Office Physical Security Policy Ledger. Office keys are additionally held by the lessor, property management, and custodial staff. These keys are not tracked by the Office Physical Security Policy Ledger. Initrobe managers regularly review physical access privileges.

Initrobe infrastructure is located within [SERVICE PROVIDER]. Initrobe does not have physical access to [SERVICE PROVIDER] infrastructure.

# **Risk Assessment**

Initrobe updates its Cyber Risk Assessment on an [ ANNUAL | QUARTERLY ] basis in order to keep pace with the evolving threat landscape. The following is an inventory of adversarial and non-adversarial threats assessed to be of importance to Initrobe.

## **Adversarial Threats**

The following represents the inventory of adversarial threats:

1. **Malware and Ransomware:** Constantly evolving malicious software poses a significant threat to the integrity and availability of Initrobe's systems.
2. **Phishing Attacks:** Deceptive attempts to acquire sensitive information, such as login credentials or financial details, through fraudulent communication.
3. **Advanced Persistent Threats:** Long-term, targeted attacks that involve sophisticated methods to breach and persist within the company's network undetected.
4. **Denial of Service (DoS) and Distributed Denial of Service (DDoS) Attacks:** Deliberate attempts to make services unavailable by overwhelming them with traffic, causing disruption.
5. **Insider Threats:** Risks arising from employees, contractors, or other internal entities with malicious intent or inadvertently causing harm.
6. **Zero-Day Exploits:** Attacks exploiting vulnerabilities that are unknown to the vendor or unpatched, making them particularly potent.

## **Non-Adversarial Threats**

The following represents the inventory of non-adversarial threats:

1. **Natural Disasters:** Events such as earthquakes, floods, or fires that can disrupt operations and damage infrastructure.
2. **Technical Failures:** Unexpected hardware or software failures that may lead to downtime or data loss.
3. **Human Error:** Mistakes made by employees, such as accidental data deletion or misconfiguration of systems, that can result in security incidents.
4. **Supply Chain Disruptions:** Issues with suppliers, partners, or service providers that could impact the continuity of business operations.
5. **Regulatory Compliance Changes:** Evolving legal and regulatory requirements that may affect how Initrobe handles and protects sensitive data.
6. **Environmental Factors:** Conditions like power outages, extreme temperatures, or other environmental factors that could affect the stability of IT infrastructure.
7. **Third-party Service Outages:** Reliance on external services, and the potential impact on operations if those services experience disruptions.

# **Access Onboarding and Termination Policy**

### Purpose and Scope:

The purpose of this policy is to define procedures to onboard and offboard users to technical infrastructure in a manner that minimizes the risk of information loss or exposure. This policy applies to all technical infrastructure within the organization.This policy applies to all full-time and part-time employees and contractors.

### 

### Background:

1. In order to minimize the risk of information loss or exposure (from both inside and outside the organization), the organization is reliant on the principle of least privilege.
2. Account creation and permission levels are restricted to only the resources absolutely needed to perform each person’s job duties.
3. When a user’s role within the organization changes, those accounts and permission levels are changed/revoked to fit the new role and disabled when the user leaves the organization altogether.

### Policy

1. *During onboarding:*
   1. User Account Creation: Create user accounts based on job roles and responsibilities.
   2. Granting Permissions: Assign permissions strictly necessary for the user to fulfill their job duties.
   3. Training on Security Policies: Provide comprehensive training on security policies, including the principle of least privilege.
   4. Multi-Factor Authentication (MFA): Enable MFA for enhanced account security.
   5. Network Access Setup: Configure network access based on the user's requirements and role.
2. *During offboarding:*
   1. Account Deactivation: Immediately deactivate user accounts upon termination or when no longer needed.
   2. Data Backup and Transfer: Ensure all critical data is backed up and transferred to relevant personnel or repositories.
   3. Revoking Permissions: Revoke all permissions associated with the user's role and responsibilities.
   4. Exit Interview: Conduct an exit interview to address any security concerns and retrieve company assets, including electronic devices.
   5. Notification of Relevant Departments: Inform IT, HR, and relevant departments of the user's departure for coordination in access termination.
3. *When an employee changes roles within the organization:*
   1. Role Change Notification: Receive timely notification from HR or relevant departments about employee role changes.
   2. Reassessment of Permissions: Conduct a reassessment of the user's permissions based on the new role.
   3. Training Updates: Provide additional security training if the new role requires different security considerations.
   4. Account Modification: Modify existing accounts to align with the updated job responsibilities.
4. *Review of accounts and permissions:*
   1. Regular Account Review: Conduct periodic reviews of user accounts and their associated permissions.
   2. Managerial Approval: Require managerial approval for any changes in permissions or access levels.
   3. Documentation of Changes: Maintain comprehensive documentation of all changes made to user accounts and permissions.
   4. Audit Trails: Implement audit trails to track and monitor changes to user accounts and permissions.
   5. Annual Security Review: Conduct an annual security review to ensure compliance with the principle of least privilege and identify any potential risks or vulnerabilities.

# **Information Security Policy**

### Purpose and Scope

1. This information security policy defines the purpose, principles, objectives and basic rules for information security management.
2. This document also defines procedures to implement high level information security protections within the organization, including definitions, procedures, responsibilities and performance measures (metrics and reporting mechanisms).
3. This policy applies to all users of information systems within the organization. This typically includes employees and contractors, as well as any external parties that come into contact with systems and information controlled by the organization (hereinafter referred to as “users”). This policy must be made readily available to all users.

### Background

1. This policy defines the high level objectives and implementation instructions for the organization’s information security program. It includes the organization’s information security objectives and requirements; such objectives and requirements are to be referenced when setting detailed information security policy for other areas of the organization. This policy also defines management roles and responsibilities for the organization’s Information Security Management System (ISMS). Finally, this policy references all security controls implemented within the organization.
2. Within this document, the following definitions apply
   1. ***Confidentiality***: a characteristic of information or information systems in which such information or systems are only available to authorized entities
   2. ***Integrity***: a characteristic of information or information systems in which such information or systems may only be changed by authorized entities, and in an approved manner
   3. ***Availability***: a characteristic of information or information systems in which such information or systems can be accessed by authorized entities whenever needed
   4. ***Information Security***: the act of preserving the confidentiality, integrity, and availability of information and information systems
   5. ***Information Security Management System (ISMS)***: the overall management process that includes the planning, implementation, maintenance, review, and improvement of information security

### Policy

1. *Managing Information Security*
   1. The organization’s main objectives for information security include the following:
      1. Protecting Confidentiality: Safeguarding sensitive information and ensuring that it is only accessible to authorized individuals within the organization.
      2. Ensuring Integrity: Maintaining the accuracy and reliability of data by preventing unauthorized alterations, modifications, or deletions.
      3. Promoting Availability: Ensuring that information and information systems are consistently available and accessible to authorized users when needed.
      4. Compliance with Legal and Regulatory Requirements: Adhering to relevant laws, regulations, and industry standards to avoid legal consequences and penalties.
      5. Protecting Customer and Stakeholder Trust: Building and maintaining trust with customers, clients, and stakeholders by safeguarding their data and sensitive information.
      6. Mitigating Risks and Threats: Identifying, assessing, and mitigating potential risks and threats to information security to prevent data breaches or unauthorized access.
      7. Facilitating Business Continuity: Implementing measures to ensure the continued operation of critical business processes and services in the face of disruptions or disasters.
      8. Fostering a Security-Conscious Culture: Cultivating a culture of security awareness among employees to reduce the likelihood of human error and promote responsible information handling.
      9. Protecting Intellectual Property: Safeguarding the organization's intellectual property, trade secrets, and proprietary information from unauthorized access or disclosure.
      10. Minimizing Financial Loss: Preventing financial losses associated with data breaches, unauthorized access, or other security incidents that may impact the organization's bottom line.
      11. Ensuring Employee Accountability: Establishing clear policies and procedures to hold employees accountable for their actions related to information security.
      12. Continuous Improvement: Implementing an ongoing process of evaluation and improvement to adapt to evolving threats, technologies, and best practices in information security.
   2. The organization’s objectives for information security are in line with the organization’s business objectives, strategy, and plans.
   3. Objectives for individual security controls or groups of controls are proposed by the company management team, including but not limited to [list key roles inside the organization that will participate in information security matters], and others as appointed by the CEO; these security controls are approved by the CEO in accordance with the Risk Assessment Policy.
   4. All objectives must be reviewed at least once per year.
   5. The company will measure the fulfillment of all objectives. The measurement will be performed at least once per year. The results must be analyzed, evaluated, and reported to the management team.
2. *Information Security Requirements*
   1. This policy and the entire information security program must be compliant with legal and regulatory requirements as well as with contractual obligations relevant to the organization.
   2. All employees, contractors, and other individuals subject to the organization’s information security policy must read and acknowledge all information security policies.
   3. The process of selecting information security controls and safeguards for the organization is defined in Reference (a).
   4. The organization prescribes guidelines for remote workers as part of the Remote Access Policy.
   5. To counter the risk of unauthorized access, the organization maintains a Data Center Security Policy.
   6. Security requirements for the software development life cycle, including system development, acquisition and maintenance are defined in the Software Development Lifecycle Policy.
   7. Security requirements for handling information security incidents are defined in the Security Incident Response Policy.
   8. Disaster recovery and business continuity management policy is defined in the Disaster Recovery Policy.
   9. Requirements for information system availability and redundancy are defined in the System Availability Policy.

## **Acceptable Use Policy**

### Purpose and Scope

This policy purpose is to define the acceptable and responsible use of the organization's IT resources, networks, and systems.

### Background In today's interconnected and technology-driven business environment, the organization relies heavily on information technology resources, networks, and systems to conduct its operations efficiently. The use of IT resources brings about numerous benefits, including enhanced communication, increased productivity, and improved collaboration. However, with these advantages comes the responsibility to ensure that the organization's IT assets are used in a manner that aligns with its values, legal requirements, and security standards.

### Given the dynamic nature of technology and the potential risks associated with misuse, it is imperative to establish clear guidelines for acceptable and responsible use.

### 

### Policy

1. Unauthorized installation of software, hardware, or other tools that may compromise system security is not allowed.
2. Email should be used for business purposes, and users should exercise caution when opening attachments or clicking on links.
3. Remote access should only be conducted through secure and authorized methods by complying with the organization's Remote Access Policy.
4. IT resources may be monitored for compliance with the AUP.
5. Users are obligated to report any security incidents, potential vulnerabilities, or suspicious activities to the IT department promptly.
6. Violations of the AUP may result in disciplinary action, up to and including termination of employment.

## **Disaster Recovery Policy**

### Purpose and Scope

### The purpose of this policy is to establish a framework for responding to and recovering from unexpected disasters or disruptions that can impact the organization's operations.

This policy covers data recovery, business continuity, and emergency response.

### Background

### In the event of a disaster this policy will ensure that the downtime of such incident will be greatly reduced.

### Policy

1. Have a team always ready to respond to such disasters
2. Always have complete backups
3. Have an inventory made of both hardware and software used

## **Password Policy**

### Purpose and Scope

The purpose of this policy is to protect access to Initrobe’s insfrastructure.

This policy should be applied to all Initrobe personnel and external contractors.

### 

### Background

We identified weak password management in initrobe’s systems. In order to improve initrobe’s authentication it is crucial to implement robust credentials.

### 

### Policy

1. Password history: password must be changed to a new and never used before password
2. Password rotation: passwords must be changed every 3 months
3. Strong passwords: passwords must be least 10 chars long

## **Remote Access Policy**

### Purpose and Scope

The purpose of this policy is to define the rules and security measures for remote access to the organization's systems and data.

### 

### Background

With the increasing trend of remote work, the need for secure connections, and potential risks associated with remote access have increased as well. Because most of the company employees work remotely we are applying this policy to make its security more harned

### 

### Policy

1. Virtual private network: A VPN is a must for secure remote connections.

## **Workstation Policy**

### Purpose and Scope

The purpose of this policy is to establish guidelines for the appropriate use and security of workstations and endpoints within the organization.

### Background

A workstation is a device, be it personal or company-owned that contains sensitive company data. It should be well protected and this policy will make sure that it is the case.

### Policy

All of the machines must be configured with the following:

1. Automatic OS updates enabled
2. Antivirus installed and scanning
3. Encrypted hard drive
4. Automatic screen lock
5. Configured to use a password manager application

## **User Automatic Lock Screen Script**

<https://github.com/Rbrasil72/Powershell-Scripts/blob/main/UserLockScreen.ps1>