Heimdal Security Compliance Whitepaper

Our commitment to Security, Compliance and Privacy

About Heimdal® Security (Heimdal/ the Company)

Founded in Copenhagen in 2014, Heimdal empowers CISOs, Security Teams, and IT admins to enhance their SecOps, reduce alert fatigue, and take proactive measures through one seamless command and control platform.

Heimdal's award-winning cybersecurity solutions cover the entire IT estate, offering solutions for every challenge, from endpoint to network level, in vulnerability management, privileged access, Zero Trust implementation, ransomware prevention, and more.

Currently, Heimdal's cybersecurity solutions are deployed in over 45 countries, supported regionally from offices in 15+ countries, by 175+ highly qualified specialists. Heimdal is ISAE 3000 certified and secures more than three million endpoints for over 11,000 companies.

Heimdal provides unwavering support to its partners, focusing on consistency and scalability. The common goal is to create a sustainable ecosystem and a strategic partnership between Heimdal and its partners.

For more information, visit Heimdal.

1. Commitment to Security

Heimdal is committed to earning and maintaining our customers' trust and confidence. Protecting our customers' data is the cornerstone of our **Information Security Program**. It is ingrained in the way we design our products, the operational security practices we put in place, the layers of protection we provide to reduce the risk, and the key legal, regulatory, and compliance certifications and attestations that we meet.

1.1. Personal Security

Prior to Employment

The Heimdal Human Resources department ensures background checks are performed for all new hires, prior to the first day of employment. Background checks generally include criminal history, education, past employment, etc. Depending on the role, new hires either sign non-disclosure agreements or have confidentiality clauses in their employment contracts. All new employees are required to review and confirm their adherence to the Heimdal employee handbook that details Heimdal's corporate policies and undertake an onboarding process.

During Employment

We maintain a Security Awareness program and an Awareness Strategy that includes mandatory training, policy acknowledgment and assessments. New employees are required to complete Security Awareness training upon being hired, and annually thereafter.

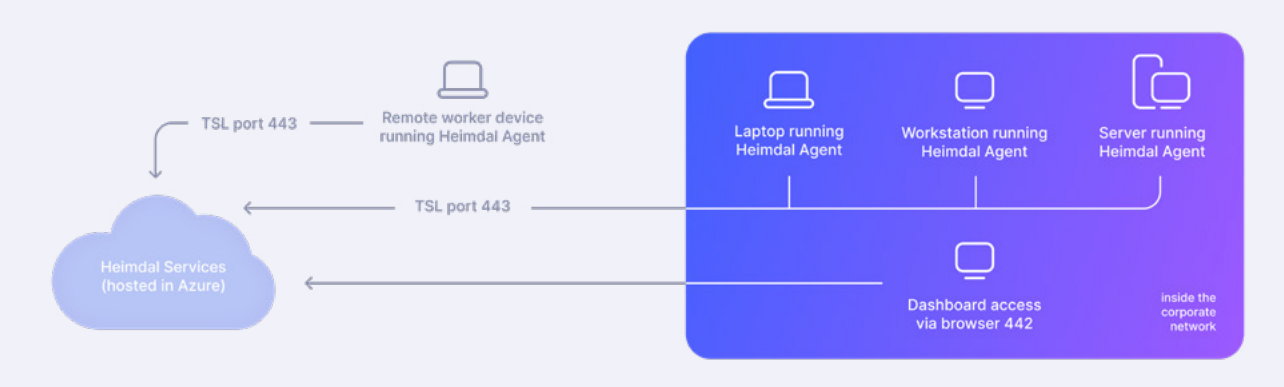
Managers are responsible for ensuring that users within their areas of responsibility apply appropriate information security controls.

Termination of Employment or Change in Role

We have developed policy controls to address the processes associated with users' terminating employment, changing job roles, or functions. We put in place processes for access revocation or modification. Employees leaving the Company are required to return all information assets belonging to Heimdal on, or prior to, their last day of employment.

1.2. Cloud Datacenter Security

Heimdal is a cloud-only environment. Heimdal does not maintain its own physical data centers or servers that contain customer data. As a result, Heimdal inherits the physical and infrastructure protections of Amazon Web Services (AWS) and Microsoft Azure (MS) cloud environments across all its servers.



Heimdal's production infrastructure is maintained by Microsoft Azure as our primary Infrastructure as a Service (IaaS) provider.

Neither AWS nor MS allow customers physical access to their data centers. For more information, please see:

- https://aws.amazon.com/security/
- https://docs.microsoft.com/en-us/azure/security/fundamentals/physical-security

Data cloud providers do not disclose **the exact addresses of their data centers**. This measure was taken to secure the data center facilities.

Cloud security is one of AWS' and MS' highest priorities. Therefore, our customers benefit from a data center and **network architecture built to meet the requirements of some of the most highly security-sensitive organizations.**

All data is stored in highly secure data centers. Both AWS and MS manage dozens of compliance programs in their infrastructure, which enables Heimdal to maintain the highest standard of security. The Heimdal infrastructure is designed to keep your data safe, regardless of your business's size.

1.3. Access Control

To manage the access across the Company, Heimdal has applied access controls to ensure that:

- access to information resources is controlled through processes that address authorization, modification, revalidation, and revocation of information system privileges.
- access is strictly limited to appropriate individuals on a **"need to know"** basis in line with their job description.
- access revocation due to resignation, termination, or transfer, is conducted in an appropriate manner.
- different users of Heimdal's information resources:
  - ✓ are accountable for all actions performed under their User ID
  - ✓ are responsible for protecting and managing the confidentiality of their passwords and log-in credentials.
  - ✓ have periodic training based on their roles and responsibilities.
- access to documents and removable media containing sensitive information is controlled.

1.4. Technical Vulnerability Management

Technical vulnerability management controls are maintained to help reduce the risks resulting from exploiting technical vulnerabilities. Exposure to new technical vulnerabilities is continually evaluated and appropriate measures are taken to address associated risks. To limit Heimdal's exposure to new vulnerabilities, **end users are not able to install unapproved software or any other software that is not work-related.**

1.5. Software Updates & Release Process

Heimdal regularly checks software capability and security requirements as part of our scheduled maintenance, releasing updates as necessary. **In the case of critical issues, Heimdal will patch or provide a fix as soon as reasonably possible.**

The release process at Heimdal is meticulously designed to ensure the utmost reliability and stability of software updates before they reach the customer environment. At Heimdal, we employ a staged deployment strategy for both our Release Candidate (RC) and Production environments, ensuring a controlled and secure rollout of new software versions.

a. **Controlled Rollout:** The rollout to both Release candidate and Production is carried out in controlled stages. This methodical approach allows us to monitor the performance and stability of the release under real-world conditions without impacting the entire network. Rollout stages are executed incrementally, typically following a sequence of small batches such as 1%, 2%, 4%, 8%, 16%, etc.

b. **Evaluation Period:** The RC version remains in this preliminary phase for a minimum period of 30 days, during which any incidents are closely monitored and addressed. Assuming zero critical incidents occur, the RC is then deemed stable for production deployment, which follows the exact same rollout methodology.

New agent deployment example*

*for illustration purposes only, not exact timeline

1.6. Data Security

Heimdal implements policies and practices to secure data processing:

Data at Rest

Heimdal databases containing customer data are **encrypted with a double layer of encryption:**

- The 1st layer is provided and managed by the cloud provider.
- The 2nd layer of encryption is fully managed by Heimdal in a completely autonomous and secure environment.

Both layers of encryption are **Federal Information Processing Standards (FIPS) 140-2** compliant and for both encryption keys we are using Advanced Encryption Standard **AES-256 (256-bit key length).**

Data in Transit

Data is only transferred as encrypted communication with TLS **(Transport Layer Security RSA SHA256 encryption)** and is **managed and controlled** fully by Heimdal. Data is always under strict access control.

Data Access

Access to information and servers is limited based on an employee's access requirements and authorization, ensuring that each employee only has access to those assets they need for executing their role and responsibilities. The principle of **"need to know"** is strictly followed while provisioning access and privileges to users. Privileges and roles that manage critical functions and processes are brought under shared responsibility with more than one person or department.

Heimdal Dashboard allows our clients to create Enterprise accounts, Reseller accounts, Distributor accounts, and Visitor accounts based on each client's need. Additionally, we provide granular Access Control Lists (ACLs) that end users can configure to manage and control access within their

organization's accounts, further enhancing security and ensuring that permissions are in line with organizational requirements.

Clients can choose not to give Heimdal access to their data in the Dashboard and our team will not have access to the client's data. For more information about the Heimdal Dashboard please access HEIMDAL Dashboard overview – Heimdal Security Assistance and Support.

2. Compliance Commitment

2.1. ISAE 3000 Soc 2 Type I and II compliant

Heimdal has committed and obtained the **ISAE 3000 SOC 2 Type I** certification in April 2021 and the **ISAE 3000 Soc 2 Type II** certification in June 2022.

Demonstrating commitment to providing customers with the highest level of data protection and security, SOC 2 reports issued under the ISAE 3000 standard are based on Trust Services Criteria for security, availability, confidentiality, processing integrity, and privacy specific principles and criteria as defined. To show adherence to each of the criteria, specific requirements must be met within the organization.

The basic goal of the Trust Services Criteria is to protect the five aspects of information:

Security: Protection against unauthorized access (physical and logical), data integrity, change management and incident management.

Availability: Availability of systems for operation and usage as agreed in the Service Level Agreements.

Confidentiality: Information designated as confidential is protected and processed accordingly.

Processing integrity: System processing is complete, accurate, timely and authorized.

Privacy: Personal information is processed and destroyed in accordance with privacy requirements of the user organization and legally required privacy requirement, such as the General Data Protection Regulation (GDPR).

In addition to security requirements, the Trust Services Criteria also contains requirements for an internal control framework, including risk management and procedures to be followed by employees to control security and data (information in systems including transaction data, databases, and individual files).

2.2. Description of Heimdal controls and Information Security Program

Heimdal has established an **Information Security Program** that provides documented management direction and support for implementing information security within the Heimdal environment. The design and implementation of applicable controls are defined based on the architecture of Heimdal's environments.

The objective of the Information Security Program is to maintain the confidentiality, integrity, and availability of information while complying with applicable legislative, regulatory, and contractual requirements.

The Information Security Program consists of the following components:

Risk assessment
Training and awareness
Security implementation
Review and compliance
Management reporting

The Information Security Program is based on the International Organization of Standards (ISO) Codes of Practice for information security management ISO / IEC 27001:2013 standard. Its policies and processes provide a framework to:

- assess risks to the Heimdal environment,
- develop mitigating strategies and implement security controls,
- define roles and responsibilities (including qualification requirements),
- coordinate different corporate departments and implement security controls based on corporate, legal, and regulatory requirements.

In addition, team-specific Standard Operating Procedures (SOPs) are developed to provide implementation details for specific operational tasks in the following areas:

Access control
Asset management
Backup and restore
Change management
Employee security
Encryption
Hardening
Incident management
IT continuity
Logging and monitoring
Patch management
Personal data preparedness
Physical security
Risk management
Software development
System management

Technical communication
Third-party management
Threat and vulnerability management
Virus protection.

2.3. Third-Party Penetration and Vulnerability Testing

A Penetration test is a set of procedures designed to bypass the security controls of a system in order to test that system's resistance to attacks.

Our products and every major release **are being tested at least once a year by an independent third party.**

Penetration tests are part of the Heimdal Information Security Program, and we believe it can benefit our Company by:

- Identifying vulnerabilities and eliminating weaknesses that could be exploited.
- Increasing resiliency against attacks to ensure continuous business operation.
- Challenging our protective strategy to make it stronger, especially for those assets that we categorized as being critical for our Company.
- Meeting industry compliance rules that are needed for operation.
- Creating a security-conscious organization.

2.4. Business Continuity and Disaster Recovery

Heimdal is dedicated to maintaining a resilient operational posture that ensures the provision of reliable and timely services to our clients, even under adverse conditions.

To support this commitment, Heimdal has developed a robust resilience program that encompasses business impact analysis, crisis management, business continuity, and disaster recovery planning:

Business Impact Analysis

At Heimdal, Business Impact Analysis (BIA) is a foundational component of the resilience strategy. The BIA systematically evaluates all critical business functions across departments, assessing the levels of criticality, associated risks, and the operational requirements necessary to sustain the delivery of key products and services. This analysis determines the recovery priorities and is integral in establishing both our Recovery Point Objective (RPO) and Recovery Time Objective (RTO). BIAs are conducted annually for each critical operational function to ensure that our resilience measures evolve in line with business and technological developments.

Incident and Crisis Management Plan

Our Incident and Crisis Management Plan outlines comprehensive measures to address and manage potential disruptive events. The plan details the activation procedures for crisis management teams, escalation triggers, and robust communication frameworks to ensure all stakeholders are informed and responsive. These processes are thoroughly tested at least annually to validate effectiveness and responsiveness.

Business Continuity Plan

Heimdal's Business Continuity Plan is designed to ensure that our critical business functions can continue during and recover quickly after any disruption. The plan specifies necessary actions regarding location, staffing, and particularly focuses on leveraging our cloud-based infrastructure with AWS and Azure to enable efficient remote work and data accessibility. This system also delineates roles and responsibilities within each team to maintain operational continuity. **Our Recovery Time Objective (RTO) for critical operations is set at a maximum of 2 hours**, reflecting our commitment to rapid recovery and minimal downtime.

Disaster Recovery Plans

Our Disaster Recovery Plans are tailored to our IT infrastructure's specifics, heavily reliant on cloud services provided by AWS and Azure. These plans detail the steps for quick restoration of IT systems and networks, specifying the necessary infrastructure, technology, and team roles required for effective execution.

The recovery strategies are tested annually, **with an established Recovery Point Objective (RPO) of no more than 24 hours**, ensuring our capability to restore operations swiftly and efficiently after any incident.

3. NIS 2 Directive Compliance at Heimdal

Heimdal is dedicated to maintaining the highest levels of cybersecurity, aligning our practices with the stringent requirements set forth by the Directive (EU) 2022/2555 — also known as the **NIS 2 Directive.** This directive, effective from December 14, 2022, mandates a high common level of cybersecurity across the Union, amending and repealing previous directives to enhance security across network and information systems.

The ISAE 3000 SOC 2 framework, which Heimdal adheres to, involves a comprehensive set of controls that are essential for ensuring data security and compliance with various cybersecurity mandates, including the NIS 2 Directive. By implementing these controls and undergoing rigorous third-party audits, Heimdal ensures that our measures are in line with the latest cybersecurity standards required under NIS 2. Key components of our Information Security Program that align with both ISAE 3000 SOC 2 and NIS 2 include:

ISAE 3000 Soc 2 control	Control activities	NIS 2 Directive Compliance
CC3.0 Risk assessment methodology	• Risk assessment	Article 21: Cybersecurity risk-management measures (a) policies on risk analysis and information system security
CC5.3 Information security policies	• Information Security Policy • Personal Data Policy • Review of policies	Article 21: Cybersecurity risk-management measures (f) policies and procedures to assess the effectiveness of cybersecurity risk-management measures

ISAE 3000 Soc 2 control	Control activities	NIS 2 Directive Compliance
CC7.0 System Operations & CC3.0 Risk assessment	• Roles and responsibilities • Remote workplaces • Authentications of external connections • Authentification of external suppliers on internal systems	Article 21: Cybersecurity risk-management measures (d) supply chain security, including security-related aspects concerning relationships between each entity and its direct suppliers
CC.1.0 Human resource security and personal	• Before employment • During employment • GDPR awareness • Non-disclosure and confidentiality agreements • End or change of employment • Communication with authorities • Control ownership and responsibili	Article 21: Cybersecurity risk-management measures (i) human resources security, access control policies and asset management
CC3.0 Risk assessment	• Risk assessment methodology • Information security risks • Risk review and approval • Ownership of assets • Classification of assets • Classification of information	Article 21: Cybersecurity risk-management measures (j) the use of multi-factor authentication or continuous authentication solutions
CC5.0 Control activities – Access management	• Policy for access management • User registration and deregistration • Management of access rights • Management of privileged access rights • Management of password requirements	Article 21: Cybersecurity risk-management measures (j) the use of multi-factor authentication or continuous authentication solutions
CC6.0 Logical and physical access controls	• Physical perimeter safeguarding • Physical access control • Data ownership • Administration of certificates and keys	Article 21: Cybersecurity risk-management measures (i) human resources security, access control policies and asset management
CC7.0 System Operations	• Vulnerability checks • Threat management • Enable detailed logging • Event alerts • Critical monitoring • Logging of unsuccessful logins • Logging of privileged access	Article 21: Cybersecurity risk-management measures (e) security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure
CC2.0 Communication and information security	• Policies and procedures for transfer of information • Track software inventory information • Information security incident management	Article 21: Cybersecurity risk-management measures (b) incident handling
CC6.2: Acquisition, development and maintenance of systems	• System acquisition, development and maintenance of systems	Article 21: Cybersecurity risk-management measures (e) security in network and information systems acquisition, development, and maintenance

ISAE 3000 Soc 2 control	Control activities	NIS 2 Directive Compliance
CC9.0: Supplier relationships, processors and sub-processors	• Agreements with sub-processors • Approved sub-processors • Supervision of sub-processors	Article 21: Cybersecurity risk-management measures (d) supply chain security
CC7.3: Information security incident management	• Information security incident management • Reporting of information and personal data security incidents • Controles and responsability	Article 21: Cybersecurity risk-management measures (b) incident handling
CC7.0:Information security aspects of disaster recovery, contingency and restore management	• Disaster recovery • Security continuity • Restore management • Business Impact Analisys	Article 21: Cybersecurity risk-management measures (c) business continuity

4. Conclusion

We emphasize Heimdal's unwavering commitment to safeguarding our clients. Our approach integrates robust security measures, strict compliance with international standards, and an in-depth understanding of privacy requirements.

We ensure that our cybersecurity solutions not only meet but often surpass the industry's highest standards, providing robust protection against evolving threats and securing the digital landscape for businesses worldwide.

It is important to recognize that achieving compliance is a shared responsibility. Heimdal's principles should be seamlessly integrated into each company's specific operational environment to enhance overall security posture.

For further details about our Security compliance and data protection practices, or if you have any specific inquiries, please contact our Compliance team at compliance@heimdalsecurity.com.

Confidentiality Disclaimer

This Whitepaper is intended for informational purposes only and is provided as a general resource, not as a comprehensive guide.

The contents are considered confidential and are the proprietary information of Heimdal. Unauthorized distribution or use of this document is strictly prohibited.

While every effort has been made to ensure the accuracy of the information contained herein, Heimdal assumes no responsibility for any errors or omissions. The information provided is subject to change without notice, and Heimdal does not guarantee that the measures described are appropriate for every situation. Specific features and details are typically provided in product datasheets and through direct consultation.

It is recommended that clients consult these resources, or contact Heimdal directly, to understand how our solutions may be configured to meet the specific requirements of their environment.

Heimdal®

HEIMDALSECURITY.COM