

Document Name: Scope of the ISMS

Document Number: 01-ISMS

Company Name:	Vanir Ventures
Policy Owner(s):	Jonah Ellinger
Effective Date:	2023-03-01
ISO 27001 Coverage	ISO 27001 4.1; 4.2; 4.3

Purpose

Vanir Ventures (The Company) has established an Information Security Management System (“ISMS”) in accordance with ISO/IEC 27001 (“ISO 27001”) that governs the processes required to protect company and information assets. This document specifies the scope of the ISMS at Vanir Ventures

Introduction

The Company utilizes the ISO 27001 Information Security (“InfoSec”) frameworks in order to identify and maintain the assets, technologies, and processes needed to protect customer information and to help ensure the confidentiality, integrity, availability, and privacy of customer data and supporting services.

To enable this, the Company:

1. Aligns its InfoSec policies and procedures to the global industry standard ISO 27001
2. Achieves a robust InfoSec framework for the efficient functioning of the organization

All locations identified including departments and assets are included in the scope of the ISMS as detailed in the following sections.

Scope of the ISMS

All offices, facilities and equipment owned and/or managed by the Company.

General

The following statement defines the scope of services for the Company:

- Online casino operation

The scope of the ISMS includes the assets, technologies and processes employed by the Company for processing, management, and delivery of services to its customers.

Additionally, the scope is defined with consideration of the external and internal context of the organization (Appendix A), requirements of interested parties (Appendix B), such as customers and regulatory bodies, and boundaries with third parties (Appendix C).

Assets

The assets of the ISMS are further categorized as information, application, database, cloud services, and Personnel. The details of the assets can be found in Appendix D.

Definitions

The definitions of important terms of the ISMS can be found in Appendix E.

Locations

All locations where work for the Company is conducted, whether remote or in an office, company provided or personal, is covered by these policies. Non-company workspaces are only covered while work for the Company is being conducted and/or Company equipment is present.

Departments

The following departments are in-scope for the ISMS:

- Information Technology (“IT”)

- Software Development (“Dev”)
- Human Resources (“HR”)
- Information Security (“InfoSec” or “IS”)
- Legal
- Operations
- Finance

Personnel

All Personnel belonging to the above departments are in-scope for the ISMS.

Scope Exclusions and Boundaries

- The Company uses a number of external IT contractors. These contractors or their companies are required to follow and maintain ISO 27001 compliance policies where needed.
- The Company uses cloud based services for hosting its services and applications.
- These service providers are responsible for managing logical access to the underlying network, system management, and storage devices for its cloud service hosting the Company's data.
- The service providers are responsible for the physical security and environmental controls at data center facilities hosting the Company's systems; therefore, physical security and environmental controls are out of scope for those facilities.
- The service providers are responsible for the secure deletion of data to support the Company's operations.
- The Company's information, application, database, facility, and Personnel assets that are not related to the identified in-scope components are out of scope for the ISMS.

External IT Contractors

External contractors are to be listed in Appendix D

Version History

Version	Date	Description	Author
1.0	2023-03-01	Initial policy	Jonah Ellinger

Appendix A - Context of the Organization

By establishing the organizational context, the Company is able to articulate its objectives, define the external and internal parameters to be considered when setting scope and risk criteria and managing risks to the objectives of the ISMS.

Internal Context

The Company established the internal context by analyzing the internal components that support the ISMS as documented below:

Internal Factors	Description
Governance	Decision making and power to define expectations and manage performance
Organizational structure	Establishment of internal hierarchy and lines of authority
Roles and accountabilities	Assignment of roles and responsibilities for the establishment, operation, maintenance, and continual improvement of the ISMS
Policies, objectives, and strategy	Processes, requirements and activities developed to achieve business objectives

Capabilities	Company resources and knowledge (e.g., intellectual property, capital, time, people, processes, systems and technologies)
Internal stakeholders	Management of perceptions, values and relationships with interested/invested parties
Organizational culture	Company values, mission statement, and employee perceptions
Information management	Information systems, information flows and decision-making processes (both formal and informal)
Internal Factors	Description
Contractual relationships	Requirements established with third parties

Interested Party	Type	Requirements
Customers	External	Protection of customer information (confidentiality, integrity, availability, and privacy) and compliance with contractual agreements
Regulators	External	Compliance with regulations and other applicable privacy laws
Business Partners and Shareholders	Internal	Protection of the Company's reputation, meeting customer expectations, and continuous generation of revenue
Employees	Internal	Information security training and awareness that can help employees align their daily operations with the Company's information security goals and objectives.
Stakeholders	Internal & External	Compliance with certification framework requirements

External Factors	Description
-------------------------	--------------------

Interested Party	Type	Requirements
Management & Board of Directors	Internal	Protection of customer information (confidentiality, integrity, availability, and privacy) and compliance with contractual agreements and external regulations. Integrity of financial reporting.

Social	The communities and customs of the environment with which the Company operates
Cultural	The shared beliefs and values of the environment with which the Company operates
Political	The governmental system(s) and practices of the environment with which Vanir Ventures operates
Legal, regulatory, and compliance	Laws, regulations, and compliance standards that may impact the Company's objectives: • EU data regulations such as GDPR • Curacao Gaming Regulations • Estonia Gaming Regulations
Financial	Allocation, management, acquisition and investment of resources in the Company
Technological	Changes in the mechanisms, processes, communications and systems used in the environment with which the Company operates
Economic	The conditions of the production, distribution, and consumption of goods of the environment with which the Company operates
Natural	The physical environment and landscape of the environment with which the Company operates
Competitive	The impact made by other companies that perform similar services
Key drivers and trends	Changes in the market that have an impact on the Company's objectives
External stakeholders	Perceptions, values relationships with key external interested parties
Contractual relationships	Requirements established with third parties

External Context

The Company established the external context through consideration of the local, regional, national, and international factors below:

Appendix B – Interested Parties and Their Requirements

The Company defines the ISMS key interested parties and their requirements as:

Appendix C – External Service Providers

The systems/organizations listed below are critical to the Company's operations. However, since the company does not have direct control over these organizations, inherent risks are reduced via a signed contractual agreement which complies with the Company's standards.

Other Organizations	Description of the Interfaces and Dependencies
Google Workspace	Availability of email, office tools, and identity and authentication platform.
Google Tag Manager	User tracking
Amazon Web Services (AWS)	Cloud hosting
Pragmatic Play Platform	Site hosting
Bright Data	VPN / proxy

Cloud Flare	Site caching, firewall, DDoS protection
Prerender.io	Prerender for search engine
Microsoft Office 365	MS Office licenses
Xero	Accounting Software
Trello	Internal project management
Send Grid	Email sending (transactional and marketing)
Payhawk	Expense tracking / company CC
Jira	eNexus / Pragmatic project management
Hot Jar	User tracking
Figma	Site Design
Atera	Remote device management

Appendix D – External IT Contractors

The systems/organizations listed below are critical to the Company's operations. However, since the company does not have direct control over these organizations, inherent risks are reduced via a signed contractual agreement which complies with the Company's standards.

Other Organizations	Description of the Interfaces and Dependencies
eNexus	Frontend development
Pragmatic Solution	Back office development/management
Rubiko	Customer support

Appendix E – Assets

Below is a detailed description of the all assets in-scope for the ISMS:

Asset Name	Description	Details
System/Cloud infrastructure	System infrastructure / Data Centers / Cloud Infrastructure	AWS Frankfurt, Maintained by eNexus
Customer data	Data stored on the Company's customers	AWS Frankfurt in Pragmatic BO
User and organization information	User information of the Company's employees	Google Workspaces
Asset Name	Description	Details
Intellectual property	Source code and company intellectual property	Google Workspace, Pragmatic BO
Operational / support procedures / system documentation	Documents that detail the operations of the ISMS	Google Workspace
Task management system (Trello)	Task management system utilized to track, maintain, and manage internal requests	Trello
Task management system (Jira)	Task management system utilized to track, maintain, and manage development requests	Jira maintain by eNexus

VPNs	For country switching / back office access	BrightData, Nord VPN, Good Access
Application websites	Websites used for customers to access the Company's service	Koicasino.com, buumi.com, joker.io
SQL Databases	Databases contain customer data	Hosted on AWS maintained by eNexus
InfoSec & IT	Personnel that are responsible for IT, system and network infrastructure.	See Organization Chart
Development	Personnel that are responsible for application development, bug fixes, and code management.	Contracted to eNexus and Pragmatic Solutions
Human Resources	Personnel that are responsible for HR policies, practices, and processes	See Organization Chart
Legal		
Finance		
Management		

Appendix F – Definitions

Below is a list of terms and definitions used throughout the Policy documents..

Term	Definition
The Company	Vanir Ventures
Personnel	All employees, contractors or other users with access to the Company's systems or equipment
IS or InfoSec	Information Security
ISMS	Information Security Management System
Information Security Manager(IS Manager)	The person responsible for the Company's overall information security
Anonymous Data	Data which does not relate to an identified or identifiable natural person.
Data Controller	A natural or legal person, Public Authority, Agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.
Data Protection Office	The person with overall responsibility for ensuring the protection of Personal Data.
Data Subject	Identified or identifiable Natural Person to which the data refers.
Identifiable Natural Person	Anyone who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
Term	Definition
Personal Data	Any information which relates to an identified or Identifiable Natural Person.

Process, Processed, Processing	Any operation or set of operations performed on Personal Data or on sets of Personal Data, whether or not by automated means. Operations performed may include collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
--------------------------------	---

Appendix G – Key Personal And Roles

Role	Name	Email
Chief Technical Officer	Jonah Ellinger	jonah@njordvantage.com
Information Security Manager	Jonah Ellinger	security@njordvantage.com
Data Protection Officer	Jonah Ellinger	dpo@njordvantage.com
Legal	Mark Idea	mark@njordvantage.com

Information Security Policy and Objectives

Document Number: 02-ISMS

Company Name:	Vanir Ventures
Policy Owner(s):	Jonah Ellinger
Effective Date:	2023-03-01
ISO 27001 Coverage	5.2;6.2

Summary

Vanir Ventures (The Company) recognise the value of information and privacy and have therefore implemented an Information Security Management System (ISMS) to control all our efforts towards Information Security.

The ISMS recognises that not all business functions within the Company are the same, and that data is used differently by various units.

By information security we mean protection of the Company’s data, applications, networks, and computer systems from unauthorized access, alteration, or destruction.

The purpose of the ISMS is:

- To protect the Company’s information assets
- To establish an operation-wide approach to information security.
- To prescribe mechanisms that help identify and prevent the compromise of information security and the misuse of data, applications, networks and computer systems.
- To define mechanisms that protect the reputation of the Company and allow the same to satisfy its legal and ethical responsibilities with regard to its networks' and computer systems' connectivity to worldwide networks.

- To prescribe an effective mechanism for responding to complaints and queries about real or perceived non-compliance with this policy. To meet Regulatory and legislative requirements.

Principles

The responsibility for all information security efforts has been appointed to the Information Security Manager (IS Manager)

Policies and procedures documents will be kept up to date and made available to all relevant stakeholders

Unless stated otherwise, these policies apply to all Personnel, internal or external, that have access to Company resources.

Information security awareness training will be provided to all Personnel.

Organizational and technical measures will be put into place to protect information assets.

Procedures will be put into place to correct and prevent any deviations and incidents.

We comply with all laws and regulations in the jurisdictions we operate in.

To provide assurance to our stakeholders, we seek compliance to ISO 27001.

Any suspected security or policy breaches should be reported to the IS Manager.

Version History

Version	Date	Description	Author
1.0	2023-03-01	Initial policy	Jonah Ellinger

Acceptable Use Policy

Document Number: 01-ISMS

Company Name:	Vanir Ventures
Policy Owner(s):	Jonah Ellinger
Effective Date:	2023-03-01
ISO 27001 Coverage	A.8.1.3

Summary

The Acceptable Use Policy (AUP) defines how Vanir Ventures's (the Company) hardware, software, systems, data and networks should be handled in day-to-day scenarios.

The policy is applicable to all Personnel, internal or external. It is to be distributed to all new Personnel before access is granted to the Company's systems.

General Guidelines

The provided credentials and login details for the Company's computers and systems must be changed upon first use.

Whenever possible a password manager should be used for password creation and ongoing management.

Credentials by the Company should only be shared using a secure communication method and only if there is no other method to provide access available. Once shared the communication must be deleted.

Any computer resources must be used in a manner that complies with the Company's policies.

The Company will monitor the use of company systems. All control system events are logged.

Unauthorized access to company systems is an offense and can lead to disciplinary action, including dismissal.

It is against our policy to install or run software requiring a license on any computer without a valid license.

Use of the Company's computer resources for personal profit is not permitted.

Decryption of passwords is not permitted, except by authorized Personnel performing security reviews or investigations.

All data contained on, or passing through the Company's assets is subject to monitoring and remains the property of the Company.

All data shared with third parties must be reviewed before sharing said data.

Under no circumstances is any Personnel authorized to engage in any activity that is illegal under local or international law while utilizing Company owned resources.

All Personnel must not use Company accounts to post publicly accessible messages or posts without permission.

All Personnel are required to access Company resources in a secure manner. Preferably using the Company provided VPN.

All Personnel are expressly forbidden to install any software on their Company provided devices without prior approval.

Whenever possible, portable media should not be connected to Company equipment and should not contain Company documents. If any portable media needs to be used, the data must be deleted as soon as it is no longer in use.

All Personnel may not perform vulnerability scans, monitor network traffic, or perform any action that is designed to escalate privileges or gain access to information that was not expressly intended for them unless required as part of their work.

All Personnel must not reveal any information about the Company's clients, employees, business practices, technology, schedules, or any other information not already publicly available to any outside resource or person without expressed permission.

All Personnel must not use their Company email accounts for purposes other than the conduct of Company business. Forbidden actions include any and all forms of harassment, phishing, solicitation, spamming, forwarding chain letters and pyramid schemes, conducting personal business, and general personal correspondence.

All Personnel must abide by the Company's Cryptography Policy.

All Personnel are responsible for their data. Any and all Company documents should be saved on the Company provided Google Drive.

Whenever possible, sharing of data should be done via Google Workspace to prevent unauthorized access or sharing of data.

All breaches of information security or any violation of the Company's ISMS policies, actual or suspected, are to be reported to the IS Manager. These reports are classified as confidential, and your input will remain anonymous.

Communication Guidelines

Any messages sent using the Company's systems are property of the Company. Messages include but are not limited to: emails, faxes, messaging services (such as Skype, Teams, WhatsApp)

The Company reserves the right to access and disclose to relevant entities the contents of all messages created, sent or received using its systems.

Sensitive data in the message or any attachments must not be transmitted in clear text..

Any urgent virus warnings should be channeled to the IS Manager for verification of authenticity.

All Personnel may not retrieve or read messages that were not sent to them unless specifically authorized by the IS Manager or by the email recipient.

Messages and copies should only be sent to those for whom they are particularly relevant.

All Personnel may not execute attachments to messages received when these are executable files (such as .exe and/or .msi);

The Company's messaging systems may not be used for personal reasons.

Accessing or transmitting pornography, posting confidential information about other Personnel, the Company or its clients or suppliers is strictly prohibited unless otherwise authorized.

An appropriate signature must be used at all times when sending emails.

Unauthorized and/or inappropriate use of Company's devices or systems may result in disciplinary action which could include summary dismissal.

All Personnel are prohibited from sharing any details of our network security or infrastructure to any 3rd party without approval from the IS Manager

Clean Desk and Clear Screen Policy

Whenever possible, physical media such as USB drives, CDs and paper should not be used to store information.

If used, physical media such as USB drives, CDs and paper should be stored in a lockable storage, including in lockable pedestals, filing cabinets and cupboards.

Computers should be switched off when not in use and must be password protected.

All Personnel are required to use a password protected screen saver that automatically fires up after only a few minutes of inactivity.

Incoming and outgoing mail collection points should be protected or supervised so that letters cannot be stolen or lost, and faxes should be protected when not in use.

All printers and fax machines should be cleared of papers as soon as they are printed.

Office, Travel & Remote Working Guidelines

The Company is remote work first. All Personnel are expected to follow the Acceptable Use Policy and other policies regardless of where they are located.

Any office where Personnel work should be treated in the same manner as remote work.

All office or home networks should be treated as a public network and assumed to be insecure.

When working from home, the Company expects all Personnel to follow all security guidelines within our policies

When working from public spaces such as airports, cafes, or hotel lobbies, it is crucial that considerations about what is visible on your screen because of where you're seated be taken into account.

Server, System and Network Policy

Personnel may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

The following activities are, in general, prohibited:

Unauthorized access to or use of data, computers, servers, systems, networks, or virtual networks, including any attempt to probe, scan, or test the vulnerability of a system or network or to breach or circumvent security or authentication measures without express authorization of the owner of the system or network.

Unauthorized monitoring of data or traffic on any network or system without express authorization of the owner of the system or network.

Interference with service to any user, host, or network including, without limitation, mail bombing, flooding, deliberate attempts to overload a system, and broadcast attacks.

Intentionally introducing malicious code, including, but not limited to, viruses, worms, Trojan horses, e-mail bombs, spyware, adware and keyloggers. Intentionally revealing one's account password or keys to others or allowing use of one's account by others.

Unauthorized access, use, probe, or scan of our system's security, authentication measures, data or traffic.

Interference with the service to any user, host or network including, but not limited to:

e-mail bombing network flooding deliberate attempts to overload the system broadcast attacks
forging of any TCP/IP packet header or any part of the header information in an e-mail or message.

Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations.

Exporting software, technical information, encryption software, or technology in violation of international or national export control laws.

Intentional misuse of any Company managed computing device, networks or resource (e.g. for cryptocurrency mining, botnet control, etc.).

Sharing your credentials for any Company managed computer or 3rd party service that the Company uses with others, or allowing use of your account or a Company managed computer by others without approval. This prohibition does not apply to single-sign-on or similar technologies, the use of which is approved.

Using a Company computing asset to procure or transmit material that is in violation of sexual harassment policies or that creates a hostile workplace.

Circumventing user authentication or security of any computer host, network, or account used by Company .

Tunneling between network segments or security zones, except when troubleshooting issues for the benefit of the Company.

Employee & Company Data

Personnel records are kept for a period of no less than 5 years after termination of contract between the Employee and the Company. All data saved on Company Managed services such as Google Workspace are property of the Company.

Messages that are created, sent or received using the Company's communication systems, including but not limited to email, Skype or Company devices, are the property of the Company.

The Company may require access to the employee’s Company communications or cloud storage after termination of contract with the employee.

Compliance Measurement

The IT Team will verify compliance to this policy through various methods, including but not limited to, business reports, internal and external audits, and feedback to the policy owner.

Any exception to the policy must be approved by the IS Manager in advance.

Any Personnel found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. In addition to Company discipline, the person may be subject to criminal prosecution under any relevant laws; civil liability; or both for unlawful use of any IT system.

If you need to report a violation of this AUP agreement or believe that you or your system has been subject to attack originating from our system, please contact the IS Manager immediately. Our team will fully investigate the situation and provide you with professional assistance.

We reserve our right to change this AUP at any time, without prior notice. We encourage our users to periodically review this Acceptable Use Policy.

ISO 27001 Coverage

ISO 27001 4.1; 4.2; 4.3

Version History

Version	Date	Description	Author
1.0	2023-03-01	Initial policy	Jonah Ellinger

Access Control Policy

Document Number: 01-ISMS

Company Name:	Vanir Ventures
Policy Owner(s):	Jonah Ellinger
Effective Date:	2023-03-01
ISO 27001 Coverage	A.9.1.1

Summary

The access control policy defines Vanir Ventures’s (the Company) rules and principles upon which access rights and restrictions are configured.

The policy is applicable to all internal and external Personnel.

Principles

The policy of the Company is to ensure that all systems and data are as secure and reliable as possible, since the entire business depends on these factors

All access is based on a 'need to know' basis.

Each member of the Company is required to understand and adhere to this policy.

Asset/system owners are accountable for ensuring that the access rights for their systems are correct.

Asset/system administrators are required to provide user accounts upon receiving authorization to do so.

The IS Manager is responsible for ensuring that Policies and procedures are adhered to within the organization.

Requirements for access control

General Guidelines

The CTO & IS Manager have the right to decline an access request on technical, operational or security grounds.

System users must agree to the Company's policies and procedures.

Each person is to have a unique login ID and associated account for accountability purposes.

Each individual is required to be accountable when accessing critical or confidential information.

Access is ideally granted via pre-defined groups based on internal company structure and role requirements. If group based access is not possible, permissions granted to the user of the system must be enough to fulfill their role and not any extra privileges.

Account creation or access changes are required to be done by the IS or IT Manager to ensure that only authorized individuals receive access to information resources.

All access privileges to information resources must be reviewed quarterly by the IS or IT Manager.

Passwords associated with logon IDs must comply with the Password Policy of the Company.

Multi Factor Authentication (MFA) should be used when possible.

The processes of terminating access must be done by the IS or IT Manager to ensure that logon IDs associated with the individual that will no longer be employed with the Company are cleared from all systems.

Approval & Pre-Approval

An approval process based on role requirements is required prior to granting access or authorization to users to make use of an information resource.

Approved default accesses for internal roles requirements are defined in the Access Matrix.

Any access to non-default systems must be requested from the IS or IT Manager.

Remote Work First

The Company is remote work first. The employee is expected to follow the Acceptable Use Policy and other policies regardless of where they are located.

Any location including company offices where an employee works should be treated in the same manner as remote work.

All office or home networks should be treated as a public network and assumed to be insecure.

Elevated Access

Elevated or Administrative access for our systems and services is only to be granted to those with a role requirement for said access.

Temporary elevated access may be requested for particular scenarios, and this may be granted for a predefined time-frame as required for the task by the IS or IT Manager

Windows Network discovery and File Sharing are disabled by default. Exceptions must be requested from the IS or IT Manager.

Administrator's Procedures

System & Application Administrators must remove accounts of individuals who are no longer authorized to have access.

They must modify a user account to reflect any necessary changes.

They must review all accounts periodically to ascertain validity.

They must also review audit trails to detect any attempts for unauthorized access.

Inactive accounts must be disabled.

Each individual that uses administrator accounts must use the account or access privilege most appropriate for the requirements of the work being performed.

Creation of User Accounts

The following procedures must be strictly adhered to before the creation of user accounts is carried out:

Any creation of new accounts must be requested from the IS or IT Manager

Any changes in Role and Access requirements must also be requested from the IS or IT Manager

System Access is granted based on the pre-approved Role Access defined in the Access Matrix.

The Access Matrix is reviewed at least annually, and changes are to be made once backed by an authorization by the appropriate level of management so as to ensure accountability.

All users must be given rights only to the data that is required in fulfilling their functions.

All users are to be made aware that they are responsible for all actions they carry out on the system.

Training should be provided on usage of the back-office system before they are allowed to access it.

Final say on access is only to be granted if endorsed by the IS Manager or CTO

Deletion of user accounts within the system - The following procedures must be strictly adhered up on employee termination:

- Any termination of employee or third party access must be requested through the IS or IT Manager
- When the termination is unplanned, a Member of the HR team must inform the IS or IT Manager of the situation immediately
- All accesses will be suspended and/or terminated on the required date and time
- Transfer of ownership of data may be requested upon termination

System Access Control List

The Access Matrix breaks down the required permissions for each of the roles within the company. This is what guides the Access Request project ticket automation.

Any non-standardised access request must be requested from the IS or IT Manager and the process is defined in the System Access & Authorization request process

ISO 27001 Coverage

ISO 27001 4.1; 4.2; 4.3

Version History

Version	Date	Description	Author
1.0	2023-03-01	Initial policy	Jonah Ellinger

Backup Policy

Document Number: 01-ISMS

Company Name:	Vanir Ventures
Policy Owner(s):	Jonah Ellinger
Effective Date:	2023-03-01

Summary

The purpose of this policy is to prevent the loss of Vanir Ventures’s (the Company) data in the case of an accidental deletion, corruption of data, system failure, or disaster to permit timely restoration of information and

business processes should such events occur, and to manage and secure backup and restoration processes as well as the media employed in the process.

This policy, and supporting procedures, encompasses all system resources and supporting assets that are owned, operated, maintained, and controlled by the Company and all other system resources, both internally and externally, that interact with these systems. 3rd Party Services such as Google are cloud based services that take care of their own data and integrity. This policy does not cover these 3rd Party Systems and Services

Policy

The frequency and extent of backups must be in accordance with the importance of the information and the acceptable risk as determined by the data owner.

Where technically feasible, automated backup procedures must be implemented to avoid the possibility of human errors. Backups must be periodically tested to ensure that they are recoverable.

Where a third party supplies offsite backup storage, the procedures between the company and the offsite backup storage supplier must be reviewed at least every six (6) months.

Any data transfer from one site to another must be carried out over a secure connection and the authenticity of both sites confirmed.

Backup log files must be kept for eventual archiving.

Version History

Version	Date	Description	Author
1.0	2023-03-01	Initial policy	Jonah Ellinger

Business Continuity Policy

Document Number: 01-ISMS

Company Name:	Vanir Ventures
Policy Owner(s):	Jonah Ellinger
Effective Date:	2023-03-01
ISO 27001 Coverage	A.17.1.2

Scope

The purpose of this document is to outline the underlying process that is inherent to all decisions taken by Vanir Ventures’s (the Company) management with regards to setting up business functions in a way that in the event of a disaster - natural or man made - the business may continue operating without issue.

Risk Assessments are to be carried out when new systems or services are being considered

General Policy

Information must be protected from a loss of confidentiality, integrity and availability.

The use of cloud services or software as a service (SAAS) is encouraged to allow business function to carry on from any geographical location.

Only pre-approved services listed in Appendix C of the Scope of the ISMS document should be used.

The services must have their own proven methods of business continuity and failover.

The services that we make use of must have adequate credential management and logging systems to prevent breaches. Backups of information used on production services must happen regularly to ensure data loss prevention.

Internal systems containing mission-critical or business data should be hosted in Amazon Web Services whenever possible.

All user day-to-day documentation or data must be kept in Google Workspace

All Personnel should only store data locally temporarily while it is in use.

All Personnel should follow the Backup Policy.

Version History

Version	Date	Description	Author
1.0	2023-03-01	Initial policy	Jonah Ellinger

Change Management Policy

Document Number: 01-ISMS

Company Name:	Vanir Ventures
Policy Owner(s):	Jonah Ellinger
Effective Date:	2023-03-01

Summary

This statement is to provide guidelines on how IT change management must happen within Vanir Ventures (the Company), and relates to any changes that are not part of the development process

General Guidelines

An initial risk assessment must be carried out to establish what information will be used or processed by the new system or role, and how the business will be affected

Depending on the results of the risk assessment, a list of checks must be created to ensure information security.

The Access Control Policy handles how any new internal system access must be handled

Any addition or change of external suppliers must provide an NDA/DPA to ensure our data is kept safe and only accessible to those that require it.

The impact of any changes to our internal network must be established before any changes take place, and said changes must be performed in such a way to minimize down time

Changes to business practices after an incident was investigated, must be based on the root-cause understanding of said incident to prevent other instances from happening

Any major changes to the Company policy must be discussed at by the management team before being taking effect

When a change is implemented a verification of the functionality of impacted systems must be performed immediately to ensure the changes were deployed successfully

Ensure all required information security policies have been met

The desired outcome of the changes must be evaluated after a set period of time, defined in the initial change request.

Version History

Version	Date	Description	Author
1.0	2023-03-01	Initial policy	Jonah Ellinger

Cryptography Policy

Document Number: 01-ISMS

Company Name:	Vanir Ventures
Policy Owner(s):	Jonah Ellinger
Effective Date:	2023-03-01

Summary

This defines when, where and how cryptography is used in Vanir Ventures (the Company), and how key management is done.

Following the Data Classification Policy, encryption must be used to protect information classified as Confidential or Sensitive, at rest or in motion.

General requirements

All Company owned laptops and workstations must have full disk encryption enabled by default.

Encryption must be used to protect Company digital data in transit by default. Any deviation from this policy must be carefully assessed by the IS Manager.

Never hard code keys during the software development or store keys outside of a secure system such as a password manager.

Limit keys to a single, specific purpose whenever possible

The keys used to encrypt data should not be stored on the same media as that data.

Requirements for certificates

The maximum duration for all certificates (signing, SSL/TLS) is 1 year

All certificates should have a key length of at least 2048 bits

Extended Validation (EV) certificates should be used for all customer facing services

Certificates should be configured to be automatically renewed. If this is not possible, alerts are used.

Requirements for keys

Encryption keys (e.g. for encryption of backups or workstations) should be stored centrally Cryptographic keys must be generated and stored in a secure manner that prevents loss, theft, or compromise.

Minimum length for RSA keys is 2048 bits

Newly generated SSH keys should use ed25519 algorithm and contain employee email `1ssh-keygen -C email@rubiko.tech -t ed25519`

Requirements for web services

All public facing web sites are scanned each quarter using ssllabs.com, a score of "A" is considered minimum
Minimum TLS version accepted is 1.2

Requirements for email

All email domains are scanned each quarter using tools such as mxtoolbox.com, found problems must be resolved

Requirements for Data sharing

Any data being shared with 3rd parties must be done via secure encrypted methods.

Any data shared with 3rd Party Auditors or Legal services must be done through singular permission access and not generic accounts It is always preferred to use a 2FA system if possible

Key Repositories

Production Platform

AWS ACM

AWS SSL Manager

For shared passwords/keys - Dashlane

Any other key that does not fall in the above 2 categories - Google Password Manager or Dashlane

Compromised keys

If a key gets compromised, contact the IS Manager. The key owner will delete the key entirely from the relevant location.

Version History

Version	Date	Description	Author
1.0	2023-03-01	Initial policy	Jonah Ellinger

Data Classification Policy

Document Number: 01-ISMS

Company Name:	Vanir Ventures
Policy Owner(s):	Jonah Ellinger
Effective Date:	2023-03-01

Summary

It is essential that all of Vanir Ventures’s (the Company) data be protected. There are however gradations that require different levels of security. All data should be reviewed on a periodic basis and classified according to its use, sensitivity, and importance

Principles

No system or network can have a connection to the Internet without the means to protect the information on those systems reflecting its confidentiality classification.

Classification	Description	Examples	Treatment
Public	Information that may be freely disseminated. Access to such information need not be controlled although specific guidelines may be issued by the Executive Team if they perceive the dissemination of such information to be harmful to the business.	Information on our public web site Brochures and leaflets	No special measures need to be taken to protect this information

Data	Internal	Information of this kind is meant to be kept internally, but no harm would be done if it would fall into wrong hands.		No special measures need to be taken to protect this information
------	----------	---	--	--

custodians are responsible for creating data repositories and data transfers which protect data in the manner appropriate to its classification.

High risk data and confidential data must be encrypted during transmission over insecure channels.

Digital data must have adequate granular access rights to prevent unauthorized access and use.

Physical copies of Confidential or High Risk data must be labeled accordingly, and kept under lock and key.

Wherever possible physical copies of data should be avoided.

All appropriate data should be backed up, and the backups tested periodically, as per the Backup Policy

Backups of data must be handled with the same security precautions as the data itself. When systems are disposed of, or repurposed, data must be certified deleted or disks destroyed consistent with industry best practices for the security level of the data.

Our organization distinguishes the following levels of information classification:

Confidential	Data that would not expose the Company to loss if disclosed, but that the data owner feels should be protected to prevent unauthorized disclosure as it would potentially pose a threat to the organization. Access to such data shall be by default given solely to employees who maintain a managerial role within the company. Access to other employees may be given on a 'need to know' basis. The dissemination of such information requires the express authorisation by a member of the Executive Team.	Personally Identifiable Information Financial information Any and all user related hardware	Information can only be shared or distributed with permission from the owner or an authorized member of the Executive Team, and when an NDA is in place. Transmission or storage should be encrypted Policies are created and shared to ensure Best Practice is enforced and followed Physical documents are stored in locked cabinets, with visible labeling
High risk	Information assets over which there are legal requirements for preventing disclosure. Data covered by local and international legislation are in this class. Payroll, Personnel, gaming, player and financial information are also in this class because of privacy requirements. This policy recognizes that other data may need to be treated as high risk because it would cause severe damage to the Company if disclosed or modified. The data owner should make this determination. Access to High Risk data must be controlled from creation to destruction, and will be granted only to those persons who require such access in order to perform their job ("need-to-know"). Access to High Risk data must be individually requested and then authorized by the Data Owner who is responsible for the data. In addition, the dissemination of such information with third parties is prohibited from doing so without the express confirmation in writing by a member of the Executive Team and preferably the right of the third party to receive such information should be prescribed in a contract.	Special categories of personal information such as Racial or ethnic origin Political opinions Religious or philosophical beliefs Trade union membership Personal health data Biometric data Sex life or sexual orientation	Information can only be shared or distributed with permission from the owner Transmission or storage must be encrypted Two factor authentication (2FA) No read access by own/maintenance Personnel Access to this kind of information must be logged and audited

Version History

Version	Date	Description	Author
1.0	2023-03-01	Initial policy	Jonah Ellinger

--	--	--	--

Customer Data Retention Policy

Document Number: 01-ISMS

Company Name:	Vanir Ventures
Policy Owner(s):	Jonah Ellinger
Effective Date:	2023-03-01

Summary

Vanir Ventures (the Company) is committed to conducting its business in accordance with all applicable data protection laws, regulations and ethical conduct standards.

This Policy sets out the expected approach in relation to the retention and deletion of any Personal Data belonging to the Company’s customers (i.e. Data Subjects).

The Company, as a Data Controller, is responsible for ensuring compliance with the rules outlined in this Policy.

Scope

The purpose of this Policy is to specify the rules for the retention of Personal Data relating to the different types of Processing activities of the Company.

This Policy applies to all forms of Processing of personal data, whether in electronic form or in manual files that allow access to information about customers.

While the need to retain certain information can be mandated by law, such data retention shall nevertheless comply with the General Data Protection Regulation (GDPR).

The retention of Personal Data belonging to the Company’s employees is not within the scope of this Policy. It is covered in the Company’s ‘Employee Data Retention Policy’.

Definitions

Anonymous Data - Data which does not relate to an identified or identifiable natural person.

Data Controller/Data Protection Office - A natural or legal person, Public Authority, Agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.

Data Subject - Identified or identifiable Natural Person to which the data refers.

Identifiable Natural Person - Anyone who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Personal Data - Any information which relates to an identified or Identifiable Natural Person.

Process, Processed, Processing - Any operation or set of operations performed on Personal Data or on sets of

Personal Data, whether or not by automated means. Operations performed may include collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Data Retention

The Company adopted this Policy to explain how it implements one of the main principles established under Article 5 of the GDPR i.e. storage limitation.

Pursuant to the 'storage limitation' principle, the Company should retain Personal Data for no longer than is necessary to fulfill the purposes for which the Personal Data is Processed.

Accordingly, upon the termination of the business relationship with the customer, the Company shall only retain customer Personal Data in accordance with the below set out rules which are based on all applicable legislation.

The Company is legally obliged to retain all customer Personal Data for the purposes of the prevention, detection, analysis and investigation of money laundering or funding terrorism activities. Such extension shall be affected if it would be considered necessary by the Financial Intelligence Analysis Unit, relevant supervisory authorities or law enforcement agencies, for the purposes of the prevention, detection, analysis and investigation of money laundering or funding of terrorism activities

The Company will follow the stricter legal requirement of all applicable legislation or the Client's policies.

In case of an ongoing legal dispute with a customer, the Company has a legitimate interest to retain the customer's Personal Data in order to manage the dispute appropriately. Accordingly, the Company shall retain all customer Personal Data until the dispute with the customer has been settled.

Data Deletion

Data deletion is a critical component of this Policy. Data deletion ensures that the Company shall use data efficiently, thereby making data management and retrieval more cost-effective, while ensuring GDPR compliance.

Upon the expiry of the retention periods specified in this Policy, the Company shall delete the relevant Personal Data. In this respect, Anonymous Data shall be equivalent to deleted data.

If a user feels that certain data should not be deleted/Anonymized, he/she should identify the relevant data to his/her supervisor, who should immediately consult the Data Protection Officer so that an exception to this Policy may be considered. Since such decisions have long-term legal implications, exceptions to this Policy shall be approved only by the Data Protection Officer.

The Company specifically directs users not to delete any Personal Data in violation of this Policy.

Version History

Version	Date	Description	Author
1.0	2023-03-01	Initial policy	Jonah Ellinger

Disaster Recovery Policy

Document Number: 01-ISMS

Company Name:	Vanir Ventures
Policy Owner(s):	Jonah Ellinger
Effective Date:	2023-03-01

Summary

The purpose of this document is to lay out the planning that the Company has carried out to ultimately ensure the smooth continuation of its business operations and should be used in conjunction with the Business Continuity Policy.

This document identifies mission critical operations as well as operations which might diminish the ability of the business to carry out its primary functions. Disruptions can be the result of a multitude of internal or external events and it is not the purpose of this procedure to detail the possible causes.

Principles

Production systems should be up within 24 hours. To achieve maximum availability, we host our production servers with AWS, in three availability zones. Uptime, backup availability and failover is checked as part of monitoring and review of supplier services

All employees should be able to remotely and do so on a regular basis.

To achieve maximum availability, we use cloud services as much as possible

Uptime and/or backup is checked with monitoring and review of supplier services

Business Impact Analysis

The following events are identified as mission critical and urgent.

An event is considered critical if the implications for stakeholders or damage to the organization resulting are regarded as unacceptable.

Perceptions of the acceptability of disruption may be modified by the cost of establishing and maintaining appropriate business or technical recovery solutions.

A function may also be considered critical if dictated by law.

Risk / Threat	Database Corruption
---------------	---------------------

Probability	Low to Medium
Impact	Medium to High
Likely Scenario	Any technical issue (i.e. bugs, overheating, hardware failure, human error)
Functions Affected	All web operations
Action	Identify the time of corruption. If replication servers are not affected, restore data from a replication server. Restore affected DB tables from last good backup if replication servers are also affected and corrupted data has already been replicated. If the whole database is corrupted, do a full restore from backup Verify restored database. Restore transactions after time of corruption using binary logs found on either production cluster machines or replication servers (remove faulty transactions if necessary) Investigate reason for corruption Ensure company is not at risk of re-corruption
Continuity Plan	Full Database backups are kept as per backup policy.
Time to resume normal operations	Normal service is expected to be resumed within 4 hours of issue.
Escalation procedure	The IT Team will inform the Management Team and then keep updated of developments. All involved technical parties are informed. The IT Team will prepare and send Incident Report with details of issue

Risk / Threat	Cloud Infrastructure / Data Center outage
Probability	Low
Impact	Low to Medium
Likely Scenario	Any hardware or connectivity issue
Functions Affected	Overall Site performance will be reduced.
Action	IT operations to Identify reason for failure with the Cloud provider Make sure all traffic is directed to healthy servers by turning off affected ones Bring servers online once cloud provider has fixed the issue
Continuity Plan	The loss of one server behind every load balancer is a survivable incident as each server has enough computational resources to handle all operations. In the case of increased traffic new servers can be also added. Furthermore, the virtual machines run in different AWS availability zones which means that an outage affecting one AWS zone is always a survivable incident.

Time to resume normal operations	Normal operations would not be affected unless a complete data center failure.
Escalation procedure	The IT Team will inform the Management Team and then keep updated of developments. All involved technical parties are informed. The IT Team will prepare and send Incident Report with details of issue
Risk / Threat	Critical Bug in Software
Probability	Low
Impact	High
Likely Scenario	Incorrectly applied update, bad configuration, etc
Functions Affected	Website operations will remain halted
Action	Identify the service and part of code causing issue Roll back to last stable version / configuration or deploy an update for the service to function correctly – whichever is the quicker
Continuity Plan	We use Docker and a microservices approach to be able to deploy rolling updates and rollbacks for our services without downtime. Updates to the services are first tested in a staging deployment and then pushed into production. In the case of a critical issue that needs to be investigated in more detail, the site will be switched to maintenance mode so that the development/engineering team can validate the bug and the fix before customers are able to access the site.
Time to resume normal operations	Website operations should be fully functional within 2 hours of issue.
Escalation procedure	The IT Team will inform the Management Team and then keep updated of developments. All involved technical parties are informed. The IT Team will prepare and send Incident Report with details of issue

Risk / Threat	Security Breach
Probability	Low
Impact	High

Likely Scenario	Access details leaked, security hole discovered and exploited
Functions Affected	Website operations will be stopped
Action	Identify entry point of intrusion Disconnect all affected systems from outside network connections or disable them entirely Assess whether any information was accessed Ensure any security hole is found and sealed before operations resume. The first step is to prevent exploiting the vulnerability with AWS Web Application Firewall rules if possible. The second
	step is to deploy a patched version of the service that is causing the issue. Inform authorities and begin tracing the source of attack
Continuity Plan	All production systems are protected by AWS Web Application Firewall (WAF) which provides us with protection for the most common attacks. WAF rules are actively monitored and updated to prevent well-known attack methods as well as custom rules specific for the Company platform. The software development method enforces security by demanding developers to follow OWASP guidelines.
Time to resume normal operations	Depending on the nature of attack. Website operations can resume as soon as the security hole is patched.
Escalation procedure	The IT Team will inform the Management Team and then keep updated of developments. All involved technical parties are informed. The IT Team will prepare and send Incident Report with details of issue

Risk / Threat	DDoS Attack
Probability	Low
Impact	Medium to High
Likely Scenario	Attempt by third party to disrupt website operations
Functions Affected	Website performance will be reduced and eventually become unavailable to customers
Action	Enable AWS protections Escalate issue to AWS and track sources of attack Customize AWS rules and/or use zone lockdown to mitigate the attack

Continuity Plan	We use AWS Cloudfront and Api Gateway to route all our publicly facing websites and API endpoints. AWS provides state of the art protection against DDoS attacks.
Time to resume normal operations	Dependant on nature and severity of attack
Escalation procedure	The IT Team will inform the Management Team and then keep updated of developments. All involved technical parties are informed. The IT Team will prepare and send Incident Report with details of issue

Risk / Threat	Office Network Failure
Probability	Low
Impact	Low
Likely Scenario	Power Outage / Hardware Failure
Functions Affected	Office Systems will be unusable
Action	Identify reason for failure, if applicable Use backup mobile internet connections If needed, relocate staff to home / area with power and internet connection, key staff able to work remotely
Continuity Plan	No systems critical to website operations are located in office. Key staff are able to work remotely from any location with an Internet connection.
Time to resume normal operations	Depending on the issue, typically several hours.
Escalation procedure	The IT Team will inform the Management Team and then keep updated of developments. All involved technical parties are informed. The IT Team will prepare and send Incident Report with details of issue

Threat analysis

Disease: The possibility of working remotely is tried and tested for these cases. This is not considered as a major threat by the company.

Earthquake: Not classified as a major threat by the company because of investment in cloud/SAAS Infrastructure which provides us with state of the art data center facilities.

Fire: Not classified as a major threat by the company because of investment in cloud/SAAS Infrastructure which provides us with state of the art data center facilities.

Flood: Not classified as a major threat by the company because of investment in cloud/SAAS Infrastructure which provides us with state of the art data center facilities.

Cyber attack: The attack would be progressively blocked closer and closer to the source. DDoS protection is also provided through AWS and international bandwidth providers.

Bribery: All employees are required to provide their police conduct. Unusual expenditures will be discreetly looked into.

Drug Use: Irrational behavior will be investigated. Employees might be required to do a drug test where allowed by law.

Hurricane: Not a major threat for the company because of investment in cloud/SAAS Infrastructure which provides us with state of the art data center facilities.

Utility outage: Not a major threat by the company because of investment in cloud/SAAS Infrastructure which provides us with state of the art data center facilities.

Terrorism: No contingency is in place for this.

Definition of impact scenarios

The ability of continued operations may be threatened. The use of cloud/SAAS infrastructure for production systems mitigates the risks involved significantly.

Recovery requirement documentation

Our cloud/SAAS systems and services are key to the company goal of being able to function with staff working from off-site locations as long as there is an internet connection. However, this flexibility does create security risks that need consideration. Our Mobile Device Policy and general InfoSec Policy guide our staff on how best to stay safe. We also make sure mission critical services are only accessible via an authorized VPN connection or whitelisted IP addresses.

The crisis management command structure

The lead in crisis management will be the CTO. If they are unavailable, command structure is CEO -> IT Manager -> IS Manager -> Most senior manager

The personal in those roles and their contact information is listed under Key Personal And Roles in the Information Security Policy

Overview Routine Testing & Maintenance

The details of the following will be periodically checked and updated accordingly upon any changes:

- Staffing changes

- Changes to important clients and their contact details

- Changes to important vendors/suppliers and their contact details

- Departmental changes like new, closed or fundamentally changed departments.

- Changes in company investment portfolio and mission statement

- Changes in upstream/downstream supplier routes

Testing and verification of technical solutions

As a part of ongoing maintenance, any specialized technical deployments must be checked for functionality. These checks include:

Virus definition distribution
Application security and service patch distribution
Hardware operability check
Application operability check
Data verification

Testing and verification of organization recovery procedures

As work processes change over time, the previously documented organizational recovery procedures may no longer be suitable. These checks are envisaged:

Are all work processes for critical functions documented?

Have the systems used in the execution of critical functions changed?

Are the documents meaningful and accurate for staff?

Do the documented work process recovery tasks and supporting disaster recovery infrastructure allow staff to recover within the predetermined recovery time objective?

Actual simulation / testing of threats identified followed by post mortem reporting will be also performed at regular intervals of not more than twelve months. This BCP will be updated to eliminate failures in procedures detected during testing.

Version History

Version	Date	Description	Author
1.0	2023-03-01	Initial policy	Jonah Ellinger

Incident Response Policy

Document Number: 01-ISMS

Company Name:	Vanir Ventures
Policy Owner(s):	Jonah Ellinger
Effective Date:	2023-03-01

Summary

This document provides the general principles for dealing with computer and non-computer incidents so that the company is always in a position to efficiently and effectively respond in a manner that protects its own information assets and helps protect the information of players that might be affected by the incident.

An incident is any event - real or suspected - that poses an actual or potential threat to the integrity of the Company's services, information, resources, infrastructure or identities. Adverse events include compromised integrity, unauthorized access (logical & physical), denial of service, compromised data, loss of accountability, or damage to any part of any system.

Policy

The Company must establish a team and procedures to address both computer incidents, including theft, misuse of data, intrusions, data breaches, and malicious software and non-computer related incidents.

Every incident must be handled in line with the policy and escalated to the responsible persons and then to the Responsible Key Person which will in turn notify any affected Clients in line with the policy and forms prescribed by the latter.

In case an information security event is a data leak or breach, the incident should be reported to the proper authorities. Where necessary a serious incident must also be escalated to the police or other relevant bodies.

Each incident must be documented. The document must contain an explanation of the type of incident, the remedial actions taken, recommendations to avoid recurrence of such incidents and any other relevant information.

Compliance

The incident handling policy and procedures are mandatory and shall be designed to standardize the Company’s actions relating to incident handling and reporting.

Negligence may lead to disciplinary action up to and including dismissal or termination of any contractual agreements

Version History

Version	Date	Description	Author
1.0	2023-03-01	Initial policy	Jonah Ellinger

Information Retention Policy

Document Number: 01-ISMS	
Company Name:	Vanir Ventures
Policy Owner(s):	Jonah Ellinger
Effective Date:	2023-03-01

Summary

The information retention policy defines the retention periods for all information in our organization.

Principles

Refer to the table below for relevant retention periods and disposal instructions for all data types:

Data type	Retention Period	Location	Disposal
Applicant data	1 year after application, only if applicant agrees to be kept on file	Digitally on Google Workspace	Delete
Financial records (invoices, tax records)	7 years	Hard-copy in locked cabinet	Shredder
		Digitally in Financial system	Delete
Personnel records (including but not limited to Contract of Employment, Personal Data Sheet, Residency/ID Cards and passports, Review Forms).	5 years after termination	Hard-copy in locked cabinet	Shredder
		Digitally in HR system	Delete
Customer records	See Customer Data Retention Policy		
Source code	Unlimited	Digitally on Gitlab	
Email	Unlimited, unless it contains any of the data types above	Digitally on Google Workspace	Delete

Version History

Version	Date	Description	Author
1.0	2023-03-01	Initial policy	Jonah Ellinger

Logging Policy

Document Number: 01-ISMS

Company Name:	Vanir Ventures
Policy Owner(s):	Jonah Ellinger
Effective Date:	2023-03-01

Summary

The logging policy defines requirements for logging and monitoring.

Principles

Logging

Recording personal information in log files should be avoided

Access to personal information should be logged where practically possible

Successful and unsuccessful login attempts to all Company systems should be logged

Log files should be protected from deletion or modification

All logging systems should be synchronized with a reputable network time provider (NTP)

Audit logs should be regularly backed up, secured, and retained for at least three months online and one year offline for all critical systems System log files are kept at least 30 days

Monitoring

Logs of servers, firewalls, routers and monitoring platforms must be reviewed on a regular basis

Access logs of servers, firewalls, routers and monitoring platforms must be reviewed on a regular basis

Usage logs of access to personal information should be monitored by the respective system owner

Monitoring of user device status, assignment, access, installed software, and baseline hardware requirements must be reviewed on a regular basis Office internet bandwidth, VPN and network hardware must be monitored for capacity management on a regular basis.

Office shared hardware such as printers, AV hardware, and any other digital device that may potentially be used to gather sensitive data must be inspected for anomalies or defects on a regular basis.

Version History

Version	Date	Description	Author
1.0	2023-03-01	Initial policy	Jonah Ellinger

Mobile Device Policy

Document Number: 01-ISMS

Company Name:	Vanir Ventures
Policy Owner(s):	Jonah Ellinger
Effective Date:	2023-03-01
ISO 27001 Coverage	4.1; 4.2; 4.3

Summary

The mobile device policy defines rules and principles for the use of mobile devices, such as laptops, tablets and mobile phones as well as work from home equipment.

Purpose

This policy defines standards, procedures, and restrictions for any and all users with legitimate business uses connecting laptops, computers, and mobile phones to Company networks, digital resources, and data. The device policy applies, but is not limited to, all devices and accompanying media that fit the following classifications:

- Smartphones
- Other mobile/cellular phones
- Tablets
- E-readers
- Portable media devices
- Portable gaming devices
- Laptop/notebook/ultrabook computers
- Wearable computing devices
- Any other device capable of storing corporate data and/or connecting to a network

In order to enforce security and remote device management, only devices that meet the following criteria are allowed to access corporate resources:

- Smartphones, tablets, and other devices running Android version 10 and higher. Smartphones and tablets running iOS 14.0 and higher.
- Laptops running Windows 10 and higher or MacOS 13 and higher

The policy applies to any mobile device that is used to access corporate resources, whether the device is owned by the user or by the organization.

The primary goal of this policy is to protect the integrity of the confidential client and business data that resides within the Company's technology infrastructure, including internal and external cloud services.

This policy intends to prevent this data from being deliberately or inadvertently stored insecurely on a mobile device or carried over an insecure network where it could potentially be accessed by unauthorized resources. A breach of this type may result in loss of information, damage to critical applications, loss of revenue, damage the company's public image, breach our data privacy requirements, and violate data privacy laws.

Therefore, all employees, contractors, or personnel using a mobile device connected to the Company's network, and/or capable of backing up, storing, or otherwise accessing corporate data of any type, must adhere to company-defined processes and policies in doing so.

Applicability

This policy applies to all of the Company's employees, including full and part-time staff, contractors, freelancers, and other agents who use any device to access, store, backup, or relocate any organization or client-specific data. Such access to this confidential data is a privilege, not a right, and forms the basis of the trust the Company has built with its clients, supply chain partners, and other constituents.

Consequently, employment at the Company does not automatically guarantee the initial or ongoing ability to use these devices to gain access to corporate networks and information.

The policy addresses a range of threats to enterprise data, or related to its use, such as:

Threat	Description
Device Loss	Devices used to transfer or transport work files could be lost or stolen.
Data Theft	Sensitive data is deliberately stolen and sold by an employee or unauthorized third party.
Malware	Viruses, Trojans, worms, spyware, malware, and other threats could be introduced to or via a mobile device.
Compliance	Loss or theft of financial and/or personal and confidential data could expose the enterprise to the risk of non-compliance with various identity theft and privacy laws.

Addition of new hardware, software, and/or related components to provide additional mobile device connectivity will be managed at the sole discretion of our IT & IS Manager. Unauthorized use of mobile devices to back up, store, and otherwise access any company-related data is strictly forbidden.

This policy is complementary to any previously implemented policies dealing specifically with data access, data storage, data movement, and connectivity of devices to any element of the company network and resources.

Responsibilities

The Data Protection Officer has the overall responsibility for the confidentiality, integrity, and availability of corporate data. The CTO has delegated the execution and maintenance of information technology and information systems to the IT & IS Manager.

Other staff under the direction of the IT & IS Manager are responsible for following the procedures and policies within information technology and information systems.

Affected Technology

Connectivity of all mobile devices will be centrally managed by the Company's IT Team and will use authentication and strong encryption measures. Although the IT team will not directly manage personal devices purchased by employees, users are expected to adhere to the same security protocols when connected to non-corporate equipment.

Failure to do so will result in immediate suspension of all network access privileges so as to protect the Company's infrastructure.

Policy & Appropriate Use

It is the responsibility of any employee using a mobile device to access corporate resources to ensure that all security protocols normally used in the management of data on conventional storage infrastructure are also applied here. It is imperative that any mobile device that is used to conduct the Company's business be used appropriately, responsibly, and ethically. Failure to do so will result in immediate suspension of that user's account.

Based on this requirement, the following rules must be observed:

Access Control

1. The IT Team reserves the right to refuse, by physical and non-physical means, the ability to connect devices to corporate and corporate connected infrastructure. The IT Team will engage in such action if such equipment is being used in a way that puts the company's systems, data, users, and clients at risk.
2. Prior to initial use on the corporate network or related infrastructure, all devices must be approved by the IT Manager. The Company will maintain a list of approved devices and related software applications and utilities. Devices that are not on this list may not be connected to corporate infrastructure. If your preferred device does not appear on this list, contact the IT Manager. Although the IT Team currently only allows listed devices to be connected to enterprise infrastructure, it reserves the right to update this list in the future.
3. Users who wish to connect such devices to non-corporate network infrastructure to gain access to enterprise data must employ, for their devices and related infrastructure, security measures deemed necessary by the IT Team. Enterprise data is not to be accessed on any hardware that fails to meet the Company's established enterprise IT security standards.
4. Devices may only access the corporate network and data through the Internet using a Secure Socket Layer (SSL) Virtual Private Network (VPN) connection. Smart mobile devices such as smartphones, tablets, and laptops will only be allowed to access corporate data through the MDM policy pushed through Google Workspace and/or Atera.

Mobile Device Management (MDM)

1. The company's IT department uses Google Workspace and Atera to enforce policies remotely. Before connecting a computer to the corporate network, the device must be set to be manageable by Google Workspace and/or Atera.
2. Google MDM (mobile device management) is used to create Work Profiles on iOS & Android Mobile Devices.
3. The mobile device management solution enables the IT Team to take the following actions on mobile devices: [remote shutdown, wipe, remote lock].

4. Atera is to be installed on all company devices to ensure our network and endpoints are protected against any sort of Viruses and/or Malware. This also allows the IT Team to monitor any potential nefarious activity and block access to potentially harmful applications, malware, and phishing attempts.
5. Any attempt to contravene or bypass the mobile device management implementation will result in immediate disconnection from all corporate resources, and there may be additional consequences in accordance with the Company's overarching security policy.
6. Upon the return of used hardware the inventory system entry must be updated, and it must be determined if the hardware meets our minimum criteria for corporate devices. If it still meets our minimum standard a full reinstallation of the Operating system must take place, followed by the standard software set installation and configuration to be fully compliant with Device Management and Security standards. If the device no longer meets minimum specification, it is wiped and removed from corporate circulation.

Security

1. User credentials and logins must be changed upon first use.
2. Employees using mobile devices and related software for network and data access will, without exception, use secure data management procedures. All data stored on the device must be encrypted using strong encryption. See the Company's Cryptography Policy for additional background. Employees agree never to disclose their passwords to anyone.
3. All users of mobile devices must employ reasonable physical security measures. Users are expected to secure all such devices against being lost or stolen, whether or not they are actually in use and/or being carried.
4. Any non-corporate computers used to synchronize or backup data on mobile devices will have installed up-to-date anti-virus and anti-malware software deemed necessary by the Company's IT Team.
5. External storage devices should not be used. Exceptions must be approved by the IT or IS Manager, and must be encrypted if they contain company data. Employees must use our Google Storage instead of physical drives.
6. Passwords and other confidential data, as defined by the Company's IT Team, are not to be stored unencrypted on mobile devices.
7. Any mobile device that is being used to store or access the Company data must adhere to the authentication requirements of the Company's IT Team. In addition, all hardware security configurations must be pre-approved by the Company's IT Team before any enterprise data-carrying device can be connected to the corporate network.
8. The IT Team will manage security policies, network, application, and data access centrally using whatever technology solutions it deems suitable. Any attempt to contravene or bypass that security implementation will be deemed an intrusion attempt and will be dealt with in accordance with the Company's overarching security policy.
9. Employees, contractors, and temporary staff accessing the Company's resources from a smartphone or tablet will NOT save their user credentials or internet sessions when logging in or accessing company resources of any kind.

10. Employees, contractors, and temporary staff will follow all enterprise-sanctioned data removal procedures to permanently erase company-specific data from such devices once its use is no longer required.
11. Employees shall seek approval prior to installation of any unauthorized software on their laptops. The IT Team reserves the right to force uninstall any software it does not deem to be safe or appropriate for use on company hardware.
12. In the event of a lost or stolen mobile device, the user is required to report the incident to the IS Manager immediately. The device will be remotely wiped of all data and locked to prevent access by anyone other than the IT Team. If the device is recovered, it can be submitted to the IT Team for re-provisioning. The remote wipe will destroy all data on the device, whether it is related to company business or personal.
13. Usage of a mobile device to capture images, video, or audio, whether native to the device or through third-party applications, is prohibited within the workplace.
14. Applications that are not approved by the IT Team are not to be used within the workplace or in conjunction with corporate data.
15. Any physical drives or data storage devices that contain company information will be thoroughly wiped or destroyed before decommissioning or handing over to 3rd parties.
16. Pre-set screen lock timers are defined by the IT Team and deployed automatically.
17. Laptops and other digital equipment must not be left unattended in cars, public transport, or be checked in as luggage.
18. Employees are to make sure that when using their mobile devices in public spaces, their screen is set up in a way to prevent “over the shoulder” information leaks.
19. Employees are advised and encouraged to take any corporate mobile device home with them at the end of day for Business

Continuity Purposes. Hardware & Support

1. The IT Team reserves the right, through policy enforcement and any other means it deems necessary, to limit the ability of end users to transfer data to and from specific resources on the enterprise network.
2. Users will make no modifications to the hardware or software that change the nature of the device in a significant way (e.g. replacing or overriding the operating system, jail-breaking, rooting) without the express approval of the Company's IT Team .
3. The IT Team will support the connection of mobile devices to corporate resources. On personally owned devices, the IT Team will not support hardware issues or non-corporate applications.
4. If devices must be sent to third party suppliers for repair, a wipe of the data must take place if possible. On devices that allow it, hard drives containing data may be removed before sending for repair. Credentials for unlocking encryption or logging into user profiles cannot be disclosed with third party suppliers.

Organizational Protocol

1. The IT Team can and will establish audit trails, which will be accessed, published, and used without notice. Such trails will be able to track the attachment of an external device to the corporate network, and the resulting reports may be used for investigation of possible breaches and/or misuse. The end user agrees to and accepts that his or her access and/or connection to the Company's networks may be monitored to record dates, times, duration of access, etc. in order to identify unusual usage patterns or other suspicious activity. The status of the device, including location, IP address, Serial Number, IMEI, may also be monitored. This monitoring is necessary in order to identify accounts/computers that may have been compromised by external parties or users who are not complying with the Company's policies.
2. The user agrees to immediately report to his/her manager, the Company's IS Manager or security@rubiko.tech any incident or suspected incidents of unauthorized data access, data loss, and/or disclosure of company resources, databases, networks, etc.
3. The Company may choose to reimburse employees if they choose to purchase their own mobile devices. Users may be allowed to expense mobile network usage costs. Reimbursement details are based on role and expected usage.
4. Every mobile device user will be entitled and expected to attend a training session about this policy. While a mobile device user will not be granted access to corporate resources using a mobile device without accepting the terms and conditions of this policy, employees are entitled to decline signing this policy if they do not understand the policy or are uncomfortable with its contents.

Policy Non-Compliance

Failure to comply with the Mobile Device Policy may, at the full discretion of the organization, result in the suspension of any or all technology use and connectivity privileges, disciplinary action, and possibly termination of employment.

The CTO and immediate manager or director will be advised of breaches of this policy and will be responsible for appropriate remedial action.

Version History

Version	Date	Description	Author
1.0	2023-03-01	Initial policy	Jonah Ellinger

Outsourcing Policy

Document Number: 01-ISMS

Company Name: Vanir Ventures

Policy Owner(s):	Jonah Ellinger
Effective Date:	2023--02-01

Summary

Outsourcing refers to an authorized person's use of a third party, irrespective of forming part of the same corporate group, to perform functions or provide services which would otherwise be undertaken by the authorized person. The third-party supplier may itself be an authorized or unauthorized person. This policy is designed to manage the risks associated with outsourcing agreements.

All authorized outsourced services are listed in Appendix C

Review and Changes

The outsourcing policy shall be independently reviewed and updated annually or when necessary, in accordance with regulatory requirements. An external and independent party may be engaged to review this policy; however, this is not strictly necessary.

Policy Statement

Authorized Persons shall ensure all outsourcing arrangements do not diminish the Company's ability to meet regulatory, contractual and/or compliance obligations. Procedures shall be identified to ensure that outsource providers employ the same standard of care in performing services as would the Company's employees.

Risk Assessments

Services and/or Functions outsourced have different impacts on the authorized person's standing, operation, compliance and performance when the outsourced activities are of 'material', 'critical', or 'key significance'.

In relation to outsourcing, specifically, the risk assessment shall take due account of the: logical and physical access to the Company's information assets and facilities required by the outsourcer to fulfill the contract; sensitivity, volume and value of any information assets involved; commercial risks such as the outsourcer's business failing completely, their failing to meet agreed service levels or providing services to the Company's competitors where this might create conflicts of interest; security and commercial controls known to be currently employed by the Company's and/or by the outsourcer.

The result of the risk assessment shall be presented to management for approval prior to signing the outsourcing contract. Management shall decide if the Company will benefit overall by outsourcing the service and/or function to the outsourcer, taking into account both the commercial and information security aspects. If the risks involved are high and the commercial benefits are marginal, the service and/or function shall not be outsourced.

Risks Associated with Outsourcing

Risks evaluated and analyzed by the Authorized Persons include:

Regulatory Risks - These risks may arise when services, products and, or activities provided by a third party fail to comply with the applicable law, regulations and license conditions governing the authorized person. While this is a broad risk, it is expected that the regulator applies more focus and weighting on 'compliance' failures of the authorized person that may ensue in the areas such as those of business integrity (such as AML measures) and consumer protection measures. The third-party service providers may be out of reach of the sphere of competence of the regulator, either with respect to regulatory remit or jurisdictional competence, or both.

Jurisdiction Risks - These risks potentially arise when an authorized person engages a service provider located in another jurisdiction, exposing the authorized person to possible economic, political and, or regulatory conditions, events and risks from the jurisdiction where the outsourcing service provider is located.

Operational Risks - Risks may arise when an outsourcing service provider exposes the authorized person to losses due to inadequate or failed internal processes/service quality or systems, or from external events or human error.

Reputational Risks - Such risks arise when the actions or poor performance of an outsourcing service provider causes the public and other stakeholders to foster a negative opinion about the authorized person and, or the licensing jurisdiction.

Other Risks - Risks presented to the Authorized Person which are specific to the outsourcing service provided.]

Protection of Personal Data and Confidentiality Agreements

1. A formal contract between the Company and the outsourcer shall exist to protect both parties. The contract shall clearly define the types of information exchanged and the purpose for doing so.
2. If the information being exchanged is sensitive, a binding confidentiality agreement shall be in place between the Company and the outsourcer, whether as part of the outsource contract itself or a separate non-disclosure agreement (which may be required before the main contract is negotiated).
3. Information shall be classified and controlled in accordance with the Company's policy.
4. Any information received by the Company from the outsourcer which is bound by the contract or confidentiality agreement shall be protected by appropriate classification and labeling.
5. Upon termination of the contract, the confidentiality arrangements shall be revisited to determine whether confidentiality should be extended beyond the tenure of the contract.
6. All contracts shall be reviewed by a lawyer for accurate content, language and presentation.
7. The contract shall clearly define each party's responsibilities toward the other by defining the parties to the contract, effective date, functions or services being provided, liabilities, limitations on use of sub-contractors and other commercial/legal matters normal to any contract. Depending on the results of the risk assessment, various additional controls should be embedded or referenced within the contract, such as:
 1. Legal, regulatory and other third-party obligations such as data protection/privacy laws, money laundering etc;
 2. Information security obligations and controls such as
 1. Information security policies, procedures, standards and guidelines, normally within the context of an Information Security Management System;

2. Background checks on employees or third parties working on the contract (in terms with sub-section "Due Diligence on Outsourcing Service Provider");
3. Access controls to restrict unauthorized disclosure, modification or destruction of information, including physical and logical access controls, procedures for granting, reviewing, updating and revoking access to systems, data and facilities;
4. Information security incident management procedures including mandatory incident reporting;
5. Return or destruction of all information assets by the outsourcer after the completion of the outsourced activity or whenever the asset is no longer required to support the outsourced activity;
6. Copyright, patents and similar protection for any intellectual property shared with the outsourcer or developed during the contract;
7. Specification, design, development, testing, implementation, configuration, management, maintenance, support and use of security controls within or associated with IT systems, plus source code escrow;
8. Anti-malware, anti-spam and similar controls;
9. Change and configuration management, including vulnerability management, patching and verification of system security controls prior to their connection to production networks;
3. The right of the Company to monitor all access to and use of the Company's facilities, networks, systems etc., and to audit the outsourcer's compliance with the contract, or to employ a mutually agreed independent third-party auditor for this purpose;
4. Business continuity arrangements including crisis and incident management, resilience, backups and Disaster Recovery. Due

Diligence on Outsourcing Service Provider

Outsourced key employees who shall be carrying out the function/service shall be subjected to background checks equivalent to those performed on the Company's employees.

Such screening shall take into consideration the level of trust and responsibility associated with the position:

- Proof of the person's identity (e.g. passport);
- Proof of their academic qualifications (e.g. certificates);
- Proof of their work experience (e.g. résumé/CV and references);
- Criminal record check;

Criteria for selecting an outsourcer shall be defined and documented, considering the:

- company's reputation and history; quality of services provided to other customers;
- regulatory status; review of recent audited financial statements; quality assurance and security management standards currently followed by the company.

Outsourcing Provider Monitoring and Oversight

1. The outsourcing service provider's financial stability and major changes in the ownership structure are to be adequately monitored by the authorized person at intervals which would reasonably ensure that the authorized person's operations are safeguarded. In certain cases, it is not possible for the authorized person to independently obtain information regarding the outsourcing service provider's financial stability or changes in ownership, and thus effective monitoring may not be possible. In such cases, the authorized person shall adopt measures such as contractual provisions whereby the outsourcing service provider is required to inform the authorized person of changes in ownership, and the authorized person's right to request the ownership structure of the outsourcing service provider, and information regarding its financial stability.

2. The authorized person shall ensure that the Company's business continuity policy is updated to cater for major changes affecting the outsourcing service provider, such as major changes in ownership, financial stability, service disruptions, expected and unexpected terminations, or unacceptable reduction in quality of service by the outsourcing provider.
3. The Company has procedures to monitor the performance of Material/Critical Business Activity service providers. The reporting framework to the Board (or relevant Committee) by the authorized person will vary depending on the type, nature and extent of risks presented by the outsourcing arrangements in which the authorized person is engaged in or intends to engage in.
4. Monitoring is conducted by the relevant authorized person and overseen by at least one Board (or relevant Committee member) to ensure there is continued focus on the respective Material/Critical Business Activity arrangement.
5. The procedures for monitoring performance must include, as a minimum:
 1. maintaining appropriate levels of contact with the service provider. This will range from daily operational contact to authorized person involvement;
 2. a procedure for the regular monitoring of the performance of the service provider against the Material/Critical Business Activity arrangement and in particular include monitoring against the service levels agreed between the service provider and the Company;
 3. a procedure for the regular monitoring of any other performance aspects of the service provider not covered under sub-paragraph above deemed to be appropriate by the Company; and where applicable, procedure to carry out the Company's site visits to the service provider.

Outsourcing Services Agreements

As a minimum any outsourcing agreement shall incorporate the following:

A description of the outsourced function or service to be outsourced;

The performance objectives of the outsourced function/service should be clearly specified;

The respective rights and obligations of the parties to the agreement are to be clearly outlined;

The outsourcing service provider's commitment to comply with all applicable laws, regulatory requirements and guidelines approved by the authorized person;

Cover the protection of personal data. In this regard, authorized persons are to ensure that outsourcing service providers maintain the same level of data protection as the former;

Allow the authorized person's compliance and internal audit departments unlimited access to its data and its external auditors full and unrestricted rights of inspection and auditing of that data;

Include an obligation on the outsourcing service provider to immediately inform the authorized person of any material change in circumstances which could have a material impact on the continuing provision of services, including but not limited to changes in the outsourcing service provider's ownership, and notification in the case of a dire financial situation faced by the outsourcing service provider, in order to provide sufficient time for the authorized person to seek an alternative without disrupting the business and its functions;

Include the terms and conditions according to which the outsourcing service provider may subcontract any of the outsourced services. Moreover, the agreement shall stipulate that in the case of subcontracting the responsibilities of the outsourcing service provider shall remain unchanged;

Contain provisions which permit the authorized person to terminate the agreement to cater for eventualities such as the transfer of responsibilities by the outsourcing service provider to another third party provider or the re-domiciliation of the outsourced function/service in house; and

Contain provisions that the outsourcing service provider can only terminate the agreement with a notice period and that such notice period is adequately long for the authorized person to seek an alternative solution.

Internal Audit

Internal Audit is authorized by management to assess compliance with all corporate policies at any time.

Internal Audit may assist with audits of outsourcing contracts including security compliance audits and report to management the risks and recommend controls relating to outsourcing.

Version History

Version	Date	Description	Author
1.0	2023-03-01	Initial policy	Jonah Ellinger

Password Policy

Document Number: 01-ISMS	
Company Name:	Vanir Ventures
Policy Owner(s):	Jonah Ellinger
Effective Date:	2023-03-01

Summary

The Password policy defines requirements for passwords and credential sharing within the Company (Vanir Ventures), as well as third party suppliers and contractors that we grant access to.

Principles

The Password Policy of the company is to ensure best practice when it comes to creation, usage, sharing, and changing of passwords. This document will help define a set of instructions for our employees to follow and for our external partners to be aware of.

Each Member of the organization is to understand and adhere to this policy

The IS Manager is to ensure systems password policies have been set on company hardware and software

Password Requirements

New employees are to be shown how the password manager(s) works, and be required to use it.

Common / shared credentials must not be used on any internal systems. If Third Parties only provide us with a single set of credentials, they must only be shared via the pre-defined vaults, and any other copies or passwords outside these vaults are strictly prohibited.

All systems which store user passwords must do so using non reversible encryption.

Users must not share usernames and passwords, nor should they be written down or recorded in unencrypted electronic files or documents. Exceptions may be allowed under specific scenarios and under specific authorisation by the IS Manager. All users must secure their username or account, password, and system access from unauthorized use.

Users are accountable for the security and use of their user accounts and passwords.

All users must have a strong password. A strong password should include a minimum length of eight characters, a mix of uppercase, lowercase, and numerical characters.

Should a user of any system forget his or her password, the password will be reset by the system administrator. The system must prompt the users to enter a new password immediately upon the first login attempt.

All passwords to systems not supporting 2FA must be changed every 90 days for security purposes.

Encrypted passwords should be enabled on any devices where it is not on by default.

Back-end systems should have an automatic inactivity log-off period of no more than 1 hour.

Users who leave their workstations must lock or log off their workstation to prevent unauthorized access. Users which fail to comply with this policy will be held liable for the use of their account and disciplinary action may be taken.

Default passwords on all systems must be changed after installation or initial sign-up.

Monitoring must be implemented on all systems including recording logon attempts and failures, successful logons and date and time of logon and logoff.

Accounts should be locked automatically after multiple password failures in any system which supports such functionality. If a system does not support such a feature, the IS Manager should regularly review the access logs of that system, to ensure that user accounts are not being mismanaged.

In the case of shared 3rd party system passwords, these must be shared using a password manager and changed when an employee with access to them no longer works with the company

Version History

Version	Date	Description	Author
---------	------	-------------	--------

1.0	2023-03-01	Initial policy	Jonah Ellinger

Physical Security Policy

Document Number: 01-ISMS	
Company Name:	Vanir Ventures
Policy Owner(s):	Jonah Ellinger
Effective Date:	2023-03-01

Summary

Since the Company (Vanir Ventures) is remote first and all work locations should be treated with the same level of care as remote work, the Acceptable Use Policy covers the employee requirements of the Physical Security Policy.

If the physical location is company provided, the office management for that location will provide guidelines for our staff to work without fear of potential compromise or insecurity.

Version History

Version	Date	Description	Author
1.0	2023-03-01	Initial policy	Jonah Ellinger

Secure Development Policy

Document Number: 01-ISMS	
Company Name:	Vanir Ventures
Policy Owner(s):	Jonah Ellinger
Effective Date:	2023-03-01

Summary

This document describes the principles and procedures for secure software development at the Company (Vanir Ventures).

Responsibilities

The lead developer is responsible for: securing the development environment against threats. the security of any given development project. overseeing the general security of the development process.
ensuring all software developers have required application security knowledge.

The software developers are responsible for ensuring that secure coding practices are followed and for reporting identified vulnerabilities. Secure system development

New technology is analyzed for security risks/vulnerabilities prior to being installed within the development architecture or the system infrastructure. Secure development guidelines should be documented and maintained for each programming language included in the development architecture.

Only approved languages may be used in software development.

Software must be designed to maintain the confidentiality of all data available and collected.

Software must be designed to be available regardless of load, and remain functional while under an attack.

Software must be designed to preserve the authenticity and integrity of all data collected and referenced.

Software must be designed so that no input is written directly into any back end system including databases.

Source code must only be stored in the Company's source code repository. No other repositories shall be used.

3rd Party Libraries

The use of libraries and frameworks is encouraged, but:

All code developed by a third party shall be tested to ensure it meets industry good practices and that it performs to meet its purpose prior to being added to the testing environment. The testing should include a review of the source code, documentation and test coverage; review of the update frequency; running local testing with the 3rd party code

The versions should be periodically assessed for vulnerabilities

Use the library or framework as-is, refrain from making changes (this makes updating a lot more complicated, and it may pose licensing problems) All externally developed routines, algorithms, or libraries in use must be properly licensed for use.

Where possible, these principles should be applied to outsourced development through contracts and supplier agreements

Secure development environment

Development, testing and operational environments must be separated and isolated.

Access controls must be in place to ensure employees can only view or edit information relevant to their job.

Development projects must be separated in a way that prevents other teams from accidentally working on items that are out of their scope.

Access to different environments and servers must be actively reviewed.

System security testing

The source code should automatically be scanned and tested for known security vulnerabilities in the development pipeline. A penetration test should be done on the operational systems regularly and always after a change in the application or system architecture.

Version History

Version	Date	Description	Author
1.0	2023-03-01	Initial policy	Jonah Ellinger

Secure Engineering Policy

Document Number: 01-ISMS

Company Name:	Vanir Ventures
Policy Owner(s):	Jonah Ellinger
Effective Date:	2023-03-01

Summary

The secure engineering policy defines rules and principles applied in design and engineering of systems, networks and infrastructure.

Principles

Network architecture and designs should always be peer reviewed

The four eyes-principle should be applied when medium and high impact network changes take place

Engineers should stay up-to-date of vulnerabilities in used networking technology (firewalls, routers, etc)

Engineers should not have access to High risk data

Servers & Databases

Databases will only store entire credit card, bank information or other payments details if the company acquires a PCI compliance certificate. The company currently stores only references to credit cards in a masked format. A PCI compliant payment gateway is used for all card processing. When possible, third-party service providers should be used for payment processing.

Publicly accessible web servers should be located on a network which is both logically separated and secured from the internal systems network. All development, testing, and production systems should be updated with the latest vendor security patches.

Deployment and Maintenance

Changes to the production environment should be authorized and logged before being implemented.

Remote maintenance accounts should be enabled when needed and disabled when the maintenance process is completed. Access to sensitive data should be logged where practically possible.

Successful and unsuccessful login attempts and the accessing of the audit logs should be logged.

System clocks should be synchronized, and log files should contain date and time stamps.

Audit logs should be regularly backed up, secured, and retained for at least three months online and one year offline for all critical systems.

Vulnerability scans or penetration tests should be performed on all applications and systems before they are put into a production environment. Before going into production, all devices must undergo a lockdown procedure where unnecessary or default services, protocols, settings, accounts, and passwords are changed or disabled.

Version History

Version	Date	Description	Author
1.0	2023-03-01	Initial policy	Jonah Ellinger

Supplier Policy

Document Number: 01-ISMS	
Company Name:	Vanir Ventures
Policy Owner(s):	Jonah Ellinger
Effective Date:	2023-03-01

Summary

The purpose of this policy is to ensure proper protection of the Company's assets that are accessed by suppliers.

Principles

Third Party Access

Third parties occasionally conduct business/provide services to the Company and thus require network communication. Access is only given to third parties after request is received from one of the Company Executives who must also specify the level of access required by such person which must be assigned by the Chief Technology Officer.

The following guidelines apply in giving access to third parties:

The third party must be covered by a contractual undertaking which binds the third party to security measures which are equivalent to the measures specified within the security policies of the Company. Where no such contractual undertaking is present, the third party must sign a declaration confirming acceptance of the security policies of the Company.

Access to third parties must respect data protection laws. The third party shall only be given access to the databases of the Company where it is absolutely necessary for the third party to have access to them given the nature of the work and service the third party must provide to the Company.

If the supplier will process PII (personally identifiable information) on our behalf a data processing agreement (DPA) must be signed and the data should be located within the EU.

Where a third party requires a remote connection to the Company's network the access control policy shall be read in conjunction with this policy. The third party's access shall be closely monitored and removed immediately when the purpose for which it was given has been exhausted.

All third party network connections will be reviewed on a yearly basis and information regarding specific third party network connections will be updated as necessary. Obsolete third party network connections will be terminated immediately.

Third party access to contracted service providers must be terminated as and when software contracts are terminated/expired. When a client or non-supplier third party requests data from us, this must be shared using secure methods to ensure data security and integrity.

Procedures surrounding risk mitigation of a supplier's access to the Company's assets must be documented, reviewed, and agreed upon by the Company and the specific supplier.

All suppliers that access, process, store, or provide various IT components must be in agreement with the Company's security requirements around suppliers' relationship with the assets.

Types of information access should be defined that different types of suppliers will be allowed, as well as monitoring and controlling the access. Types of obligations applicable to suppliers should be defined to protect the organization's information.

Security requirements agreements for suppliers must also include details on addressing risks surrounding the handling, processing, and communicating of assets or services.

Processing facilities from business processes involving external parties shall be identified and appropriate controls implemented before granting access.

Legal and regulatory requirements, including data protection, intellectual property rights, and copyright, etc. should be clearly identified and addressed.

Supplier Service Delivery Management

A process must be developed to monitor and assess the service delivery of a supplier to ensure it is meeting appropriate business and security requirements, as well as meeting any contract or SLA requirements.

A change management process must be in place to address any alterations to an existing policy, including documentation of said change and ensuring it is in alignment with business processes and follows appropriate re-assessment of risk involved, if necessary.

ISO 27001 Coverage

ISO 27001 4.1; 4.2; 4.3

Version History

Version	Date	Description	Author
1.0	2023-03-01	Initial policy	Jonah Ellinger

Testing Policy

Document Number: 01-ISMS

Company Name:	Vanir Ventures
Policy Owner(s):	Jonah Ellinger
Effective Date:	2023-03-01

Summary

The testing policy describes rules and principles on how testing is applied in our organization.

Type Responsibilities

Testing should be done at multiple stages of development, using multiple types of testing:

Testing Type	Responsibility	Notes
Unit Testing	CI / Developer	Unit tests are run automatically during continuous integration. Test failure causes deployment failure.
Static Application Security Testing	CI / Devops	SAST performed using ?? and related tools for the platform code and reports vulnerabilities. Failure is reported if there are any new vulnerabilities. Checks are run both manually and via CI. Javascript code is checked by an internal scanner, our custom ruleset and external dependency check for node.js modules. The findings will be treated according to the treatment of vulnerabilities.
Integration Testing	Developer	Integration tests using databases are run automatically during continuous integration. Test failure causes deployment failure.
Component testing	Developer	Component tests in the framework would test the public API of a service. This test type is not yet implemented.
Manual/Whole System Testing	QA	This is done by humans as described in the change management process.
E2E Testing	Developer & QA	Continuous integration of the front end projects runs end-to-end tests automatically and reports failures via email. E2E testing for the platform is not yet implemented.
Verification And Validation Testing	QA & Product/Ticket Owner	This is done by humans as described in the change management process.
Load Testing	Developer & QA	Ideally QA handles this completely with guidance from the developer who implemented the feature. Not done in continuous integration.

Regression Testing	QA	We do not do automatic regression tests but unit tests should catch most regression related bugs. Micro services help to minimize regression bugs. Manual regression testing is done when QA is testing new features.
Penetration testing	Devops	We perform penetration tests monthly on our production websites using OWASP's Zed Attack Proxy (ZAP). External penetration testing is conducted yearly. The findings will be treated according to the treatment of vulnerabilities.

Scoring

Vulnerabilities should be scored according to the Common Vulnerability Scoring System (CVSS), version 2 or 3

Exceptions to the CVSS score (e.g. related to impact calculation) should be agreed upon with the penetration tester involved. If arbitration is needed, a second opinion can be obtained from another penetration testing company.

Treatment of vulnerabilities

CTO can allow exceptions to the treatment if the finding is deemed as false positive which happens sometimes with automatic tools.

Severity	CVSS 2	CVSS 3	Treatment
None	-	0.0	None
Low	0.0-3.9	0.1-3.9	Added to the backlog for next version
Medium	4.0-6.9	4.0-6.9	Following the Incident management process
High	7.0-10.0	7.0-8.9	Following the Incident management process
Extreme	-	9.0-10	Following the Incident management process , should be fixed immediately

Environment Testing

When it comes to tickets/changes to the frontend, they must be tested on multiple combinations of devices and environments.

Device	Browser	Notes
Windows Desktop	Edge, Chrome, Firefox	
Mac Desktop	Safari, Chrome, Firefox	
IPhone	Safari, Chrome, Firefox	Multiple screen sizes and generations should be tested
Android Phone	Edge, Chrome, Firefox	Multiple screen sizes and generations should be tested

Test Case Format

Field	Description
Summary	Describe the test case objective
Steps	The exact steps which will be performed in the test case
Preconditions	The conditions that must be in-place/followed before the test case is executed
Automated	If this test case is a manual or automated test
Status	PASS or FAIL
Notes	Any remarks/notes about the testing the test case

Version History

Version	Date	Description	Author
1.0	2023-03-01	Initial policy	Jonah Ellinger

Data Breach Response Procedure

Document Number: 01-ISMS

Company Name:	Vanir Ventures
Policy Owner(s):	Jonah Ellinger
Effective Date:	2023-03-01

Summary

The purpose of the policy is to establish the goals and the vision for the data breach response process. This process will clearly define to whom it applies and under what circumstances, and it will include the definition of a breach, staff roles and responsibilities, standards and metrics (e.g., to enable prioritization of the incidents), as well as reporting, remediation, and feedback mechanisms.

The policy shall be well publicized and made easily available to all Personnel whose duties involve data privacy and security protection.

The Company's Information Security intentions for publishing a Data Breach Response Policy are to focus significant attention on data security and data security breaches and how the Company's established culture of openness, trust and integrity should respond to such activity.

The Company's Information Security is committed to protecting Customer Data, Company's employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

This procedure mandates that any individual who suspects that a theft, breach or exposure of Personally Identifiable Information has occurred must immediately provide a description of what occurred to the Information Security Manager and/or the Data Protection Officer.

If these individuals are unable to be reached, anyone from Management can be informed instead.

GDPR - Definition of a Breach

A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

Examples of personal data breaches provided by the European Data Protection Board can include:

- access by an unauthorized third party;
- deliberate or accidental action (or inaction) by a controller or processor;
- sending personal data to an incorrect recipient;
- computing

devices containing personal data being lost or stolen; alteration of personal data without permission; loss of availability of personal data.

Definitions

Data Subjects - Data subject refers to any individual person who can be identified, directly or indirectly, via an identifier such as a name, an ID number, location data, or via factors specific to the person's physical, physiological, genetic, mental, economic, cultural or social identity.

Personally Identifiable Information (PII) - Any data that could potentially identify a specific individual. Any information that can be used to distinguish one person from another and can be used for de-anonymizing anonymous data can be considered

High Risk data - As per our Data classification policy: Information assets over which there are legal requirements for preventing disclosure. Data covered by local and international legislation are in this class. Payroll, Personnel, gaming, player and financial information are also in this class because of privacy requirements. This policy recognizes that other data may need to be treated as high risk because it would cause severe damage to the Company if disclosed or modified. The data owner should make this determination.

Roles & responsibilities

The Company Executive Team has overall administrative authority and must be consulted throughout the incident response process.

The Company Incident Response Team (IRT) has the overall operational responsibility for data breach response. The Lead of the IRT is composed of the Data Protection Officer and/or IS Manager.

Depending on the incident the IRT Lead will involve any of the contacts within the contact list within this document and possibly directors, managers, employees, lawyers, law enforcement officers, players, contractors etc. Specific tasks will be allocated by the IRT as part of the incident handling process. All people involved in the incident response and clean-up are responsible for providing any needed information to the IRT.

The IS Manager shall ensure that all incidents are handled in line with the policy and procedures and that all the Company employees shall be properly advised of their roles and responsibilities and the procedures to be adhered to.

The IRT will investigate all reported thefts, data breaches and exposures to confirm if a theft, breach or exposure has occurred. If a theft, breach or exposure has occurred, the Data Protection Officer will report the incident to the Information and Data Protection Commissioner.

The Responsible Key Person shall liaise with the clients to ensure that it is timely and fully informed in the manner it requires Data Breach handling procedures

As soon as a data breach of the Company's Protected or High Risk data is identified, the process described below is followed. A data breach is always classified as an incident of extreme severity. See Incident Severity in the Incident management process. Stage 1 - protection of the system / operation;

This stage is the preventive and detective processes in place by the Company in line with the information security and other policies and procedures.

A key part of this stage is the incoming alerts and reporting which could be the point of origin of occurrence/detection of an incident.

Accordingly all Personnel must be on the alert for any situations/information highlighting a possible incident. After an initial assessment a decision whether the IRT Lead members should be notified or not must be taken.

Stage 2 - identification and analysis of the problem;

At this stage the IRT Lead is involved if not already so.

The IRT members are chosen based on the event type and platform breached.

The IRT classifies the incident as an Extreme event.

Identification of the Type of data that was affected

Identification of the Data Subjects that were affected

Ascertain if PII's were disclosed

The IRT performs a risk assessment and develops a containment, eradication, recovery, and investigation strategy (mitigation plan). In certain cases the IRT Lead may deem necessary obtaining the approval of the Company Executive Team before proceeding.

As the process continues, the IRT may update the analysis. In practice, the Analysis, Containment, Eradication, and Recovery phases may overlap and iterate.

Stage 3 - containment of the problem in line with mitigation plan;

The IRT may quickly make an initial announcement for limited distribution to the affected parties to inform them that an incident response is in progress and to request information about any services that may be affected.

The IRT may prepare multiple announcements for affected parties to direct and inform the containment process.

IRT Lead may deem necessary obtaining Company Executive Team approval prior to sending announcements.

The IRT monitors the scope of the (ongoing) incident.

The IRT may request revocation of certificates, blacklist of users, disabling of accounts, update to firewall rules, shutdown of services, etc.

As incidents may spread across sites, areas of responsibility, the IRT must coordinate as appropriate with ISP, Payment Processors, Responsible Key Person and other affected parties.

Stage 4 - eradication of the problem in line with mitigation plan;

The IRT works with ISP, software providers, Payment Processors and others to eradicate the vulnerability by updating software, modifying system configurations, leaning/restoring compromised systems/accounts, etc.

Once more announcements may be deemed necessary by the IRT and approvals may be sought by the IRT Lead. Stage 5 - recovering from the incident and the follow-up analysis.

All systems are restored to a normal mode of operation, affected users obtain new credentials, if required, and accounts and services are re-enabled

Once more announcements may be deemed necessary by the IRT and approvals may be sought by the IRT Lead.

Stage 5 - Closure & Follow-Up

The IRT writes a summary and plans post-mortem activities. All involved parties should meet and discuss actions that were taken and the lessons learned. All existing Policies and Procedures should be evaluated and modified, if necessary. A report should follow and recommendations escalated for approval, implementation and amendment of this document where necessary.

Inform the appropriate people as listed in Appendix G

Filing of incident at the Relevant Authorities

The Data Protection Officer must report a data breach to the Information and Data Protection Commissioner within 72 hours of the incident Information security incidents are to be reported to the Clients no later than 72 hours of the incident.

Develop a communication plan

Work with communications, legal and human resource departments to decide how to communicate the breach to: internal employees

- Data Subjects directly affected
- the public

Version History

Version	Date	Description	Author
1.0	2023-03-01	Initial policy	Jonah Ellinger

Hardware Decommissioning Procedure

Company Name:	Vanir Ventures
Policy Owner(s):	Jonah Ellinger
Effective Date:	2023-03-01

Summary

This process describes the steps to be taken when hardware is decommissioned. This would happen when the hardware fails to meet our minimum specifications or requirements for it to fulfill its role or if it is to leave the control of the Company's IT Team.

Procedure

When possible, hardware is collected by the IT Team. If not possible, the employee will certify that the hardware was decommissioned correctly.

Once, the hardware is received:

Assets inventories are updated to reflect the current status and reason the hardware is to be decommissioned

HDD/SSD drives are securely wiped in line with secure wiping process using Disk Wipe

Remote wiping is used in some cases via Google MDM on devices that are not readily accessible.

The hardware is stored in a secure location, awaiting decision on decommissioning.

Hardware is donated, sold, or recycled

The hardware in question might not meet the minimum specifications for the company, but might be suitable for personal use. If the device meets the above conditions, we would decide on a case-by-case basis how to sell or donate the device in question. If the hardware is beyond economical repair, we would engage an authorized 3rd party supplier to dispose of the hardware securely.

Version History

Version	Date	Description	Author
1.0	2023-03-01	Initial policy	Jonah Ellinger