Information Security Policy

Expense Management.
Simplified. For you.

FINDITY

Document version	Approved version date	Review
7	2023-04-25	2023-04-25
Information Classification	**Owner**	**By**
Internal	DPO	DPO

Findity AB
556838-8200
findity.com
info@findity.com

Expense Management.
Simplified. For you.

Document version	Approved version date	Review
7	2023-04-25	2023-04-25
Information Classification	Owner	By
Internal	DPO	DPO

1 Introduction

FINDITY and its subsidiaries develop and supply digital financial services within a receipt and expense management framework.

Information is one of FINDITY'S most important assets and its management is an extremely important part of the work Findity does. "Information assets" refers to any information owned by FINDITY, customers, or partners, whether processed manually or digitally and regardless of its format or the environment in which it is located.

The Information Security Policy is defined by the DPO and sets out Findity's fundamental approach and commitment of purpose at an overall level regarding information security work.

Overall, this is Findity's policy document for information security work at a strategic level. Based on this governing document, instructions and playbooks are created in areas of the organization that, at a tactical and operational level, describe how the work is done and by whom.

2 Definition

Information security is about providing FINDITY's information assets with the correct protection over time and it covers the following aspects of security:

- Availability - that information is available to the expected extent and within the requested time
- Accuracy - that information is protected against unwanted and unauthorized alteration or destruction
- Confidentiality - that information not in breach of legal requirements or local agreements/guidelines is made available or withheld as unauthorized
- Traceability – in retrospect, to unequivocally link specific activities or events to an identified object or user (who, what, when)

3 Information classification

Classification is used to promote proper controls for safeguarding the confidentiality of information. Regardless of classification the integrity and accuracy of all classifications of information must be protected. The classification assigned and the related controls applied are dependent on the sensitivity of the information. Information must be classified according to the most sensitive detail it includes. Information recorded in several formats (e.g., source document, electronic record, report) must have the same classification regardless of format. The following levels are to be used when classifying information:

- Confidential Information

Confidential Information is very important and highly sensitive material. This information is private or otherwise sensitive in nature and must be restricted to those with a legitimate business need for access.

Examples of Confidential Information may include: personnel information, key financial information, proprietary information of commercial sponsors, system access passwords and information file encryption keys.

Unauthorized disclosure of this information to people without a business need for access may violate laws and regulations, or may cause significant problems for Findity, its customers, or its business partners. Decisions about the provision of access to this information must always be cleared through the information owner.

- Internal Information

Internal Information is intended for unrestricted use within Findity without advance permission from the information owner. Internal information is not to be distributed to external parties without a well motivated decision and a proper NDA in place. Unauthorized disclosure of this information to outsiders may not be appropriate due to legal or contractual provisions.

Examples of Internal Information may include: personnel directories, internal policies and procedures, most internal electronic mail messages.

Any information not explicitly classified as Confidential or External will, by default, be classified as Internal Information.

- External Information

External Information has been specifically approved for public release by a designated authority within each entity of Findity. Examples of External Information may include marketing brochures and material posted to Findity entity internet web pages.

This information may be disclosed outside of Findity.

4 Responsibility

Responsibility for FINDITY's information security work shall comply with normal, delegated, operational responsibility at all levels.

- The board expresses the principles and commitment of purpose by setting out FINDITY's information security policy.
- The management team is ultimately responsible for FINDITY's information security work and sets out the Information Security Guidelines. The management team manages and is responsible for FINDITY's infrastructure, services, systems, and applications and appoints information and system managers to them.
- Each department manages and is responsible for its own business-specific infrastructure, services, systems, and applications, and appoints information and system managers for these.
- All employees are responsible for maintaining information security and reporting incidents.

5 Management of information security incidents

There is a well defined process surrounding incident management. Everyone should be alert to and report events that have happened previously, are currently happening or could affect the safety of our information assets according to the Incident management process. Improvement measures should be clearly reported and documented to prevent future occurrences of a similar nature.

At the sensitive nature of the incident, the evidence shall be collected, preserved and presented when needed. This is stated in Incident Management Policy.

6 Focus

Information security work at FINDITY is characterized by:

- knowledge of how information security is ensured,
- continuous analysis and maintenance of crisis management capacity,
- continuous analysis of the threat to information assets,
- prevention of events that could have negative consequences, and
- information security work being a natural part of the business.

7 Services and infrastructure

7.1 Application operations, software and services development and maintenance

FINDITY uses SCRUM (see: http://www.scrumguides.org) to govern development processes. JIRA (https://findity.atlassian.net) is used to manage the team's backlog, including new features and bug management. A sprint lasts a minimum of three weeks and ends on a Wednesday; a sprint demo is held on Wednesday and is followed by a production deployment. Iteration planning is held the following Thursday.

7.2 The delivery model

The delivery model includes:

- Development – locally in each development environment
- Testing – a shared internal test environment for internal integration and function tests
- Stage – a shared test environment for end partners.
- Production – a dedicated production model for partners and end users

7.3 Support systems

The following support systems are used for development:

- Source code management: GitLab on an internal server accessible via VPN
- Build environment: GitLab on a dedicated server

7.4 Patch management

Patch management includes controls for vulnerabilities, patches, and fixes against package management systems, 3:d-party source code repositories and vulnerability lists. Patch management is manual and includes a review of all physical and virtual machines once a week at a minimum.

System patching includes evaluating available patches and manually applying them to affected systems.

7.5 Physical security

FINDITY's system is deployed at dedicated data centers. The data center service provider limits physical access to Finditys pre-registered authorized personnel from the Operations Team. Registration is required for admission. Perimeter security consists of intrusion, fire/smoke, and water alarm systems, video surveillance, code locks, and physical locks.

7.6 Redundancy

The server environment consists of multiple and redundant physical servers in separate rack cabinets with associated separate disk cabinets for storage. Each rack is physically locked to prevent unauthorized access. Each server and network equipment has redundant power, network interfaces, and cooling without any single point of failure.

The network infrastructure consists primarily of redundant, physically separated switches and redundant network cards in each server. Internet connectivity via redundant connections provided via separate ISPs and physical connections. The data centers are connected via redundant fiber links.

7.7 Power supply

The data centers use a redundant power supply which is backed up by diesel generators in the event the main power supply is disrupted. Each physical server, switch, firewall and disk cabinet has a redundant power supply fed via redundant PDUs that are backed up by UPS for battery operation.

7.8 Destruction of storage media

Destruction of unneeded storage media containing sensitive information is by multiple overwriting followed by physical destruction by a trusted third party, where the destruction is documented by the third party.

7.9 Communications and operations

FINDITY's services are operated within its own infrastructure in the form of physical and virtual servers and networks. Separate services are served from separated physical servers.

7.10 External network connections

External network connections are hardened and configured to protect against unauthorized traffic. All external connections to the services are made through a DMZ and registered in an auth log. Tagged VLANs separate internal networks (for instance but not limited to TEST, DMZ, PROD, Admin and OOB Management) where external traffic is separated from internal traffic by a firewall and separate VLANs.

Externally, only ports 25 (inbound mail receipts), 80, 443 (HTTP/s), and 1194 (UDP for VPN) are open for incoming traffic. Outgoing traffic is allowed over ports 22, 80, 443, 7590 (backup), 9418 (source code management) and 2196 (Apple Push).

7.11 System access and logging

Access control lists, authentication, and encryption using VPN Access Server in the DMZ provide backend security. Only system operators have backend access and are registered on the VPN Access Server. System operators are allowed system network access only from equipment provided by the company. Backend access requires 2-factor authentication. All activities through shell access are logged.

All traffic goes through the DMZ. Local auth logging of all login attempts to the backend takes place in the DMZ. Authentication logging for production systems and services takes place in the log server on each application server as well as the central log server.

The central log server is separated from all other systems. Read access to logs is granted to the entire operations team, but root access to the log server is limited to Findity's Security Manager.

7.12 Encryption

All communications to and from FINDITY's services, system to system or program to program, transmitted external to the backend, are encrypted. Information transmitted between the Internet and the backend is encrypted using HTTPS/SSL or SSH. Public TLS certificates for FINDITY.COM are issued by LetsEncrypt.

Data at rest in server environments are encrypted on file system level using zfs encryption.

All workstations and laptops must use full disk encryption.

7.13 Malware checks

Checks to detect and prevent malware from running are carried out regularly using rootkit detection and removal tools. IDS/IDP monitors for malware over time.

Office workstations and laptops have installed anti-virus and anti-malware software.

7.14 Information sharing

FINDITY handles sensitive financial information and must prevent unauthorized access to external or Internet-exposed applications and their information. Partners' data are protected using access control lists in order to prevent unauthorized access to information where it is processed on shared servers. Firewalls separate web and application servers from database servers. Public web servers are also separated from application and database servers in the backend by a DMZ.

Servers are not allowed to access USB devices without explicit action from a system administrator.

7.15 System access

Access to the production system's backend is only possible through wired networks and encrypted connections (VPNs). Access to the backend is granted based on functional requirements for the service and is limited to those resources required to meet the company's needs. Connections to backend services require authentication and encryption over OpenVPN and FortiGates FortiClient respectively.. Access to backend operating systems requires SSH (with keys). Only System Administrators within the Operations team are allowed system access (Admin network, Lights-out network, File system and Physical/Virtual OS access).

The exchange of credentials (such as usernames, passwords, and digital certificates) between clients and applications on networks may not be sent in clear text and must be transmitted over different systems.

No host/system may use default passwords for any account. Default passwords must be changed immediately upon installation and passwords must not be guessable using dictionary attacks. If the host or system supports non-keyable passwords, all default accounts should be assigned non-keyable passwords. Otherwise all default passwords must be changed to a random password of at least 30 characters.

7.16 Event logs

Event logs are generated for systems and networks used within the service's framework and are stored for at least 45 days. Event logs can be analyzed for security-related events. Event logs for accounts with privileged access to the backend are logged and analyzed in a separate system, see *7.1.1 Systems access and logging*.

7.17 Subcontractors

Hired subcontractors only have access to those parts of the services that are necessary for the subcontractors to be able to perform the service or services they have been hired to do. Subcontractor access is regulated by access control lists, authentication, and encryption using a VPN Access Server in the DMZ and through dedicated VLANs for the relevant services.

7.18 Backup

Backups are made exclusively to ZFS-based disk systems and are done at several distinct levels.

File system development has focused on data integrity, that is, the protection of information on storage media against bit rot, phantom writes, etc.

- Backups run locally with redundancy to separate disks across physical servers.
- Local ZFS snapshots of application servers and databases are taken every hour.
- A full ZFS backup is run every night between datacenters.
- Results are logged in the file system journal. Markup is done using timestamps.
- Redundant disaster recovery backup takes place over VPN to dedicated backup volumes at a different physical location. The DR backup is encrypted, both in transit and at rest.
- Backup volume integrity is verified weekly using zfs scrub command.
- Backed-up data integrity is further verified by performing recovery from backup.

8 Miscellaneous

8.1 Risk assessments and vulnerability analysis

FINDITY regularly conducts risk assessments and vulnerability analysis using the OWASP Top 10 as the minimum requirement level.

3:d-party penetration testing shall be performed at a minimum annually.

Continuous vulnerability scanning using automated tools shall be performed on all product services including, networks, physical and virtual hosts at least weekly.

Detected vulnerabilities shall be mitigated by order of severity:

Severity	**Mitigation**
Critical/Highest	Immediately (max 2 days)
High	Within the next sprint. (max 42 days)
Medium	Within six sprints (max 126 days)
Low	When feasible

FINDITY

Document version	Approved version date	Review
7	2023-04-25	2023-04-25
Information Classification	**Owner**	**By**
Internal	DPO	DPO

Revision history

Revision number	Created date	Created by	Approved date	Approved by
1	2019-03-15	Henrik Wejdmark	2019-05-29	Stefan Cohen
2	2019-08-08	Maria Ollinen	2019-08-08	Stefan Cohen
3	2019-11-28	Henrik Wejdmark	2019-11-28	Stefan Cohen
4	2021-05-24	Stefan Cohen	2021-05-24	Stefan Cohen
5	2021-06-24	Henrik Wejdmark	2021-08-31	Stefan Cohen
6	2022-09-20	DPO	2022-09-20	CTO
7	2023-04-25	Henrik Wejdmark	2023-04-25	CTO