INFORMATION SECURITY POLICY

INTRODUCTION

FINDITY and its businesses, Companyexpense and Digitalreceipts, 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 management team and sets out Findity's fundamental approach and commitment of purpose at an overall level regarding information security work.

This document, Information Security Policy - Services and Infrastructure, sets out the approach to information security, overall objectives, and the organization's intentions regarding information security work.

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

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)

RESPONSIBILITY

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

- The owners express 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.
- The information security coordinator works on behalf of the management team. The information security coordinator has the overall and strategic responsibility for leading, developing, and coordinating information security work.
- 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.

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.

SERVICES AND INFRASTRUCTURE

APPLICATION OPERATIONS, SOFTWARE AND SERVICES DEVELOPMENT AND MAINTENANCE

FINDITY uses SCRUM (see: http://www.scrumguides.org) to govern development processes. Pivotal Tracker (https://www.pivotaltracker.com) is used to manage the team's backlog, including new features and bug management. An iteration lasts a minimum of two weeks and ends on a Wednesday; an iteration demo is held on Wednesday. Iteration planning is every other Thursday.

THE DELIVERY MODEL

The delivery model includes:

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

SUPPORT SYSTEMS

The following support systems are used for development:

- Source code management: GIT on an internal GIT server
- Build environment: Jenkins on a dedicated server

PATCH MANAGEMENT

Patch management includes controls for vulnerabilities, patches, and fixes. Patch management is manual and includes a review of all physical and virtual machines once a week.

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

PHYSICAL SECURITY

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

REDUNDANCY

The server environment consists of several physical servers in separate rack cabinets with associated separate disk cabinets for storage. Each server has redundant power, network cards, and cooling.
The network infrastructure consists primarily of redundant, physically separated switches and redundant network cards in each server.

POWER SUPPLY

The data center uses a redundant power supply which is backed up by diesel generators in the event the main power supply is disrupted. Each physical server and disk cabinet has a redundant power supply and is also backed up by UPS for battery operation.

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.

COMMUNICATIONS AND OPERATIONS

FINDITY's services are operated exclusively within its own infrastructure in the form of physical and virtual servers

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 (TEST, DMZ, PROD) 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).

SYSTEM ACCESS AND LOGGING

Access control lists, authentication, and encryption using OpenVPN Access Server in the DMZ provide backend security. Only system operators have backend access and are registered on the VPN Access Server.
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 Graylog on each application server and with redundancy.

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 SPARAKVITTOT.SE and FINDITY.COM are issued by DigiCert.

MALWARE CHECKS

Checks to detect and prevent malware from running are carried out regularly using rootkit detection and removal tools.

INFORMATION SHARING

FINDITY handles sensitive financial information and must prevent unauthorized access to external or Internet-exposed applications and their information. Partners' data are separated into unconnected database tables and 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.

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 Cisco AnyConnect respectively (in development). Access to backend operating systems requires SSH (with keys).
The exchange of credentials (such as usernames, passwords, and digital certificates) between clients and applications on networks has been implemented so that account details and passwords/keys are transmitted over different systems.

EVENT LOGS

Event logs are generated for systems and networks used within the service's framework and are stored for at least 180 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.

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 OpenVPN Access Server in the DMZ and through dedicated VLANs for the relevant services.

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. Such problems can, among others, manifest themselves by the data on the hard drives spontaneously starting to change and becoming incorrect, without any intervention from a user or operating system, or as the result of mechanical or external factors such as cosmic radiation or power surges. ZFS provides very good protection against bit rot and other data corruption and also includes built-in backup functionality.

- Backups run locally with redundancy to separate disks across two physical servers.
- Local ZFS snapshots of application servers and databases are taken every hour.
- A full ZFS backup is run every night.
- Results are logged in the file system journal. Markup is done using timestamps.

- Redundant remote backup takes place over SSH to dedicated backup volumes at a different physical location.
- Backup volumes are verified weekly using the ZFS zpool scrub command.
- Backed-up data integrity is verified regularly by performing recovery from backup.

MISCELLANEOUS

RISK ASSESSMENTS AND VULNERABILITY ANALYSIS

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

Security reviews of the production system are carried out by a trusted third party using standardized intrusion prevention tools. The results of the security reviews are documented separately and placed in a backlog for prioritization according to assessed risk.

The current architecture and implementation are deemed robust with regard to redundancy and backup procedures. However, there is no geographical redundancy and we intend to address this as soon as possible.

SYSTEM DOCUMENTATION

System documentation is secured using authentication and encryption over HTTPS. Access is limited solely to employees in the development department.