IT AND INFORMATION SECURITY POLICY

Readly International AB (publ)

Org. No. 556912-9553

Document name	IT and Information Security Policy
Version	1.2
Latest review	18 November 2021
Document location	Readly Intranet
Document prepared by	Joakim Johansson (CTO)
Document approved by	BoD (14 December 2021)

Table of Contents

1 Introduction

1.1 Purpose & objectives

The objective with this policy ("**IT and Information Security Policy**") is to ensure that Readly International AB ("**Readly**") complies with applicable laws and regulations and that Readly's way of working with information and IT security is valid throughout the organisation.

This policy regulates how Readly manages information and information technology ("**IT**") security and also privacy.

This policy applies to Readly International AB and its subsidiaries (**the "Group**") as applicable. When using "**Readly**" in this Policy, this should be read as any company in the group or the group as a whole.

1.2 Regulatory requirements

External rules and legislation that are relevant for Readly's IT operations and systems and processing of information include:

- Data protection such as the General Data Protection Regulation ("**GDPR**").
- General guidelines regarding information security and IT operations such as Industry standards ISO 27001 are also relevant for Readly.
- External industry standards that are relevant for Readly IT such as PCI Self-Assessment Questionnaire ("**PCI SAQ**").

1.3 Policy Owner and responsibility for approval

The BoD is responsible for adopting, evaluating and reviewing this policy. This policy should be adopted annually, or more frequently if any amendments are required.

The CTO is the Policy Owner and responsible for the content of this policy. This policy is reviewed on an annual basis in order to ensure compliance with internal and external requirements. It can also be reviewed due to change in Readly business objectives, change in risk environment or change of regulatory requirements

1.4 Monitoring of policy compliance

The CTO is responsible for communicating its content and ensuring Readly's adherence to this policy.

2 IT and Information Security Policy

This policy shall set out comprehensive guidelines for information security, IT security and privacy governance at Readly.

A distinction is made between IT security, which constitutes the processes and controls for handling information in the IT services, systems, infrastructure and databases ("**IT Services**"), and information security, which encompasses all handling of information and data ("**Information Assets**") at Readly.

2.1 IT Document structure

This policy, alongside the IT Policy, are the steering policies for the Readly IT organisation ("**Readly IT**").

3 IT Security

IT security is an integral part of information security and shall ensure appropriate protection of business-critical IT Services and Information Assets.

Readly uses IT security industry standards to protect Information Assets. This includes virus protection, network protection, identity and access management, safe storage, handle deviations, activity logging and intrusion detection system.

Guiding principles for the management of IT security:

- To enable effective IT security governance the Readly IT Service Inventory shall indicate the level of business-criticality of each listed IT Service.
- Business-critical IT Services have appointed Service Owners.
- Access control shall be used to ensure that only intended users have access to IT Services and information.
- For protection against unauthorised access all employees are restricted to only use granted usernames. Employees are personally responsible for safekeeping of usernames and passwords and for not, intentionally or unintentionally, sharing these with anyone else inside or outside Readly.
- All workstations/computers and devices connected to the network must have antivirus protection that is regularly updated.
- The possibility to work remotely shall be enabled by protecting IT with appropriate security measures.
- Security incidents is managed according the Incident Management Instruction
- Password settings for business-critical IT Services shall be validated against IT Policy and the Readly Password Instruction.
- Third party agreements for business-critical IT Services shall specify appropriate security standards are met and be able to report on compliance. Readly should have right to audit when deemed necessary.

4 Information Security

Information security shall protect business operations and employees by defining appropriate information security requirements, based on applicable legislation, best practice and any complementing risk assessments performed.

Guiding principles for the management of information security:

- To protect confidentiality, integrity and availability of information. Best practice shall be applied based on appropriate parts of the ISO/IEC 27001 standard.
- The most business-critical IT Services and Information Assets shall be identified and classified to ensure that an appropriate level of security is applied.
- There shall be an appropriate level of traceability regarding creation, use, change and deletion of information depending on classification.
- Information shall only be stored as long as legal and internal requirements demand it.

- Premises and technical facilities shall be protected by appropriate physical security measures.
- Third party agreements for IT Services shall specify appropriate security measures for information security, incident management, data breach reporting and privacy rights. Readly should have right to audit when deemed necessary.

4.1 Information Classification

In order to protect Information Assets all information and IT Services are subject to Readly's information classification ("**Information Classification**"). The classification is protected with access control according to the Identity and Access Management Instruction.

Levels of classification:

Classification	Description	Examples
1. Public	Anyone is permitted and intended to have access to the Readly Information Asset, including all of Readly and external parties.	• Publicly published information about Readly. • Shareholder information (annual reports, minutes of the general meeting). • Public website
2. Internal	Access is restricted to all identified Readly staff. Information Assets are not intended for external parties without business justification.	• Policies • Confluence • Open Google Team Drives
3. Restricted	Access is restricted to those who have a business justification to receive and access the Information Asset. *A security breach is expected to cause badwill among customers and clients, the public, employees and/or other parties, and have a major negative impact, financially or otherwise.*	• Default for Readly Information Assets • "All Company" update and strategy work • Google drive with access limited appropriately • IT Service: Readly Backoffice, CRM (Braze), Reporting tool (Tableau)
4. Confidential	Highest security level. Access is restricted to those who have a business justification to receive and access the Information Asset. *A security breach is a critical incident that affects Readly's business and requires notifying the affected stakeholders and/or relevant authorities.*	• Financial report before official statement • Identifiable and confidential employee information (legal, illness) • IT Service: Unit4, Söderberg & Partner, SLT-mgmtGsuitDrives

5 Privacy rights and GDPR

Readly shall comply with applicable data protection legislation in all countries where Readly has operations, in order to safeguard that privacy rights are not violated. The IT and Information Security Policy shall be applied to ensure that appropriate security measures are implemented to protect personal data, based on how sensitive it is. Processes and IT Services shall be designed to ensure compliance with the data protection legislation.

Appropriate steering documents shall be in place, so that Readly is able to demonstrate compliance with relevant data protection legislation in case of an audit request from the Data Protection Authorities. This is essential in order to avoid sanctions. Further details are contained in the Policy for Processing of Personal Data

Definitions

BoD	Board of Directors of Readly International AB
CTO	Chief Technology Officer
CFO	Chief Financial Officer
Policy Owner	The member of senior management responsible for the policy
Service Owner	The employee accountable for an IT Service at Ready

Policies, instructions and other relevant documents

Below is a specification of policies, instructions and other documents relevant to this policy. All policies are to be reviewed on an annual basis and kept in compliance with external regulations.

- Policy for Policies
- Risk Policy
- Internal Controls Policy
- IT Policy
- IT Service Management Instruction
- Identity and Access Management instruction
- Change Management Instruction
- Incident Management Instruction
- IT Service Inventory
- IT Disaster Recovery Plan
- IT Controls Framework
- Policy for Processing of Personal Data

- Password Instruction

Appendices

None