r2p Data Security Policy
for external user access to r2p SaaS environments

Valid for Horizon Hosted Services

1 Introduction

1.1 Purpose

The r2p data security policy for external user / access represent a common understanding of data and information security and the given access to r2p SaaS (Software as a Solution) environments.

r2p regards a high level of security not only as a requirement for complying with legal and regulatory requirements, but also as a quality element in providing a secure service to cooperating partners, authorities and professionals and our customers

We understand data and information security to mean the necessary protection of all resources that are included in or contribute to r2p's processing and communication of data electronically, etc. including technology and organisational processes.

External User with an approved access to r2p SaaS environments are obliged to follow the regulations listed in this document.

2 Access control

2.1 Account handling and control

Access to and activities on r2p SaaS systems are monitored continuously based on IT internal guidelines and procedures.

2.2 User and Supervisor Responsibility

The named user who has received access to the contractual r2p SaaS and its named account manager or supervisor are responsible for:

- Not to share their accounts information or given passwords
- Logins and passwords are treated confidentially and must not be disclosed.
- Secure handling of account and password information
- Immediate notification to r2p in case of any doubt of a lost or abuse of the login
- Immediate notification to r2p if the named user left the customers company

2.3 User Access Management

r2p reserves the right to take action in case of misuse or conspicuous behaviour of access to the SaaS environment

- Run specific monitoring against the account
- Lock the access in case of abuse or conspicuous behavior
- Notify the customers listed supervisors on abuse or conspicuous behavior

2.4 Client Management

r2p expects that the r2p customers are using approved IT client systems or IT devices that meet the common security standards.

- patched client (Windows, iOS, Linux, Android) operating systems (OS)
- patched applications and web browsers
- installed approved and active antivirus solutions