RFS CYBER SECURITY STATEMENT

In an ever-increasing digital landscape, cyber security is of the highest importance. At RFS we understand the importance of a security strategy that protects the confidentiality, integrity, and availability of data both for us as a company, and our customers.

We have a robust security strategy in place that implements numerous measures at every level across the organization. This commitment to security is designed to limit the risk of cyber threats and to provide our customers with the assurance that their data is being handled with the utmost care and in line with all data protection regulations.

INFORMATION SECURITY STRATEGY

- Annual review of Cyber Security risk assessment and action plan
- Contingency planning to ensure business continuity
- Full incident response plan to limit impact in the event of a breach

TECHNICAL SECURITY

- Back-up power supply for all data centers
- Built-in resilience via redundant WAN connectivity
- Redundant server
- Spatial separation of data storage and backup (including SAP)
- Secure VPN access to all resources within RFS network
- Frequent backup of all critical server and databases
- Encryption for laptops
- Roll out of MFA for access to cloud applications

THREAT PROTECTION

- Firewalls implemented WAN gateways
- MS endpoint protection against malware
- Regular security patches, virus definition, and firewall update

ORGANIZATIONAL SECURITY

- Annual, mandatory Cyber Security awareness training for end-users
- Updated warnings based on recent attacks to ensure security is front of mind for our team
- Named user access control to applications