Radar

Information Security Policy - Radar Group

Owner (Role): Management Radar Group
Written by: Coen Ran
Status: Approved
Last Update: 04-10-2024
Next Scheduled Review: Q3 2025 (Privacy Policy Cycle)

Information Security Policy for You

This policy is a company-wide security policy explaining your responsibilities as an employee of Radar regarding information security.

About this Policy

Radar collaborates with citizens, professionals, and clients to build an inclusive, diverse, resilient, and just world. Radar aims to drive movement and change. We ask the people and organizations we work with to be open and vulnerable, as change cannot occur otherwise. Therefore, people and organizations must trust that Radar is a safe and efficient partner.

Security encompasses availability, integrity, and confidentiality. As our organization becomes increasingly dependent on technology, we prioritize securing it properly. This also aligns with the growing requirements from clients and legal regulations.

The goal of this information security policy is to ensure business continuity and prevent security incidents. If an incident does occur, this policy aims to minimize its impact.

Information security is everyone's responsibility. Managers play a leading role and set the example for good information security practices within their teams.

---

1. Basic Rules

I. We handle customer and colleague information with care.
II. Considering information security is an integral part of your work at Radar.
III. To enable business operations and innovation, we implement security measures that are effective and proportional to the risks we aim to manage.

2. Login and Accounts

Multi-Factor Authentication (MFA) is mandatory for all systems used within Radar. If a system required for work does not support MFA, a risk assessment is conducted before use, and additional measures may be taken as necessary. The system owner is responsible for this process.

Access to Microsoft 365 Environment Employees receive login credentials to access Radar's Microsoft 365 environment. This includes a login name with a Radar email address, a temporary password, and a second factor (an authentication app on the phone).

Employees must create a new password following these rules:

- The Radar password must not be stored in password managers, browser autofill, or written on paper.
- The Radar password must not be shared with anyone, including colleagues. If someone else needs access to your data (e.g., email), delegated access must be arranged through IT.
- The Radar password must not be used for other accounts.
- The password must not contain personal information, such as birthdays or family/pet names.
- If the password is forgotten, or if an employee suspects it has been compromised, they must reset it immediately via https://aka.ms/sspr.

Other Passwords If employees receive login credentials from a client, they must follow the client's security policy. If no policy exists, at minimum, a unique password must be used and not written down.

Employees may also require login credentials for work-related third-party services (e.g., online retailers). Such passwords should be unique and securely stored. RadarICT provides the password manager 'Keeper' as the standard solution. Managers must assess whether employees need access and request it from IT.

When an employee leaves the company, all access is revoked. If responsible for a system containing user accounts, employees must ensure accounts are blocked or removed upon an employee's departure.

3. Digital Workplace

Radar's IT department is responsible for securing the Microsoft 365 environment, ensuring employees can work securely with their accounts, associated devices, and applications.

Employees must:

- Use company-approved tools and not introduce personal or unauthorized tools.
- Follow guidelines available on Radar's internal pages regarding ICT and privacy.
- Consult IT before using new tools or apps outside of RadarICT's management.
- Adhere to additional security measures for specific activities or projects.

---

4. Physical Workplace

Clear Desk / Clear Screen Policy Employees must secure work materials when stepping away from their desks. Papers must be stored in locked cabinets, and documents organized properly. Avoid presenting sensitive data on screens during meetings.

At the Office

- Lock computers when stepping away (shortcut: Windows + L).
- Shut down laptops when not in use to activate encryption.

On the Go

- Adjust work practices to ensure security in public spaces.
- Avoid discussing sensitive matters in public (e.g., on trains).
- Do not leave work materials unattended.
- Avoid public Wi-Fi; use a mobile hotspot instead.

At Home

- Follow the same security protocols as at the office.
- Use Radar-issued devices and accounts.
- Ensure work materials are stored securely.

---

5. Handling Equipment

Employees must handle company-provided devices with care and follow RadarICT’s instructions.

- Use provided protective cases and bags.
- Private use is allowed within reason but should not interfere with work.
- IT may remove non-essential software during troubleshooting.

Company devices are registered in the AFAS system upon issuance.

---

6. Secure (Online) Communication

Employees must ensure information is transmitted securely and reaches the correct recipient.

- Do not open unknown attachments.
- Verify sender identities.
- Avoid unnecessary group emails.
- Report suspected phishing attempts to RadarICT.

6.1 Emails Sent on Behalf of Radar

- Use mass email tools (e.g., Postera, Mailchimp) for emails to 50+ recipients.
- Use BCC for large group emails.
- Avoid using company email for personal matters.

6.2 USB Sticks and External Media

- Files transferred to USB must be deleted afterward.
- Use encrypted USB drives secured with BitLocker.
- Never insert unknown USB sticks into company laptops.

6.3 Paper Documents

- Minimize unnecessary printing.
- Secure printed materials appropriately.
- Use shredders or secure disposal bins for sensitive documents.

6.4 Digital File Transfers

- Standard email is not secure for sensitive files.

- Follow client instructions for secure file transfers.
- Use encrypted email or secure file-sharing solutions.
- Invite external users to Teams when collaboration is needed.
- Avoid WeTransfer; use KPN Secure File Transfer instead.

This policy ensures Radar maintains a high standard of information security, protecting both company and client data. If in doubt, contact RadarICT for guidance.