Data Protection and IT Usage Policy

Responsible Entity

Schirm GmbH
Geschwister-Scholl-Straße 127
39218 Schönebeck (Elbe)
Germany
Phone: +49-3928-456-199
Fax: +49-3928-456-300
E-mail: schirm@schirm.com

Management Board

Thomas Schulz

Data Protection Officer

FKC CONSULT GmbH
Eschenburgstr. 5
23568 Lübeck
Phone: +49 451 400510
E-mail: Datenschutz@schirm.com

IT / System Administration

Sascha Kirchhoff
Schirm GmbH
Geschwister-Scholl-Straße 127
39218 Schönebeck (Elbe)
Phone: +49 3928 456325
Mobile: +49 172 7088032

Foreword

For Schirm GmbH (hereinafter referred to as “the company”), the secure handling of personal data belonging to customers, employees, business partners, and service providers is of strategic importance. As an employee, you make a significant contribution toward maintaining this objective.

The following document defines the internal guidelines for the secure processing of personal data. Employees commit themselves, by means of an additional declaration to the employment contract, to comply with data protection regulations within the company.

General Information

The company’s IT systems are intended exclusively for business use and solely for the purposes defined in the employment contract.

Employees are provided with fully preconfigured work equipment to perform their duties, including:

- Internet access
- E-mail access
- Mobile phones
- Mobile devices
- Laptops
- PCs
- Tablets

No unauthorized modification of configurations is permitted.

The IT department is generally available on working days from 7:00 a.m. to 8:00 p.m. Outside these hours, maintenance work and system restart may occur at any time.

Employees are required to cooperate and communicate with the IT department conscientiously, comprehensively, and truthfully.

Employees are personally liable for intentional misconduct, gross negligence, or criminal offenses.

These regulations also apply when using company IT outside company premises.

---

1. IT Usage

1.1 Private Use of Company IT

Employees are prohibited from using company IT for private purposes in any form.

This particularly includes:

- Downloading, storing, or editing private documents

- Using private storage devices
- Private use of browsers or internet-enabled software
- Sending or receiving private messages, images, or videos via e-mail, chat, messenger services, or similar communication software
- Accessing, distributing, or storing content that violates personal rights, copyright law, data protection law, or criminal law
- Unauthorized downloading or sharing of copyrighted content such as music, films, or software
- Accessing or distributing defamatory, discriminatory, racist, extremist, sexist, violent, or pornographic content
- Distributing malware, viruses, or engaging in attacks on IT systems
- Accessing paid online services without managerial approval
- Distributing religious, ideological, or political content
- Publishing opinions or information related to the company without authorization

The following are also prohibited:

- Unauthorized hardware or software changes
- Independent installation of software or apps
- Use of IT for non-business purposes
- Disclosure of confidential information or trade secrets
- Private deliveries to the company address
- Circumvention of security systems
- Charging private devices via company USB ports
- Use of private IT devices within the company network

The company reserves the right to conduct random checks or further investigations in cases of suspected misuse.

The camera function of private devices must be disabled when entering company premises. Photography within company premises requires approval from a supervisor.

1.2 Handling and Maintenance

Company IT equipment must be handled carefully and cleaned regularly using approved materials.

Maintenance work may only be performed by the IT department.

Defects must be reported immediately.

Employees may not attempt repairs independently except for simple visual checks.

1.3 Business Communication and E-Mail Access

Private use of the company e-mail account and e-mail programs is prohibited.

Employees must:

- Verify recipients before sending information

- Exercise caution with auto-complete recipient lists
- Use CC and BCC correctly
- Use only company-provided communication systems
- Never forward business information to private accounts or cloud services
- Share personal data only where legally permitted

Incoming and outgoing electronic messages are archived automatically in accordance with statutory retention obligations.

Regular backups of e-mail accounts are also created.

Selective deletion of private messages is technically impossible. Therefore, compliance with the prohibition of private e-mail use is also in the employee's own interest.

1.4 Mobile Devices

Employees using company mobile devices must:

- Not install software independently
- Protect devices with passwords
- Store devices securely
- Use external networks only with VPN enabled
- Report loss or damage immediately
- Avoid permanent local storage of company data
- Protect devices from unauthorized access
- Enable encryption wherever possible

1.5 Printers

Printouts must be collected immediately.

Special care must be taken with sensitive documents such as personnel files.

Misprints must be destroyed securely.

Printing should only occur when digital processing is not possible.

1.6 Files

Personal data files must be processed on designated network drives.

Local storage is permitted only in exceptional cases.

1.7 Telephone / Fax

No personal data may be disclosed during unauthenticated calls.

Private use of telephone and fax systems is prohibited.

1.8 Attachments

Unknown or suspicious e-mails with attachments must never be opened and should be deleted immediately.

The IT department should be informed if necessary.

1.9 Spam

The company uses spam filters for unwanted e-mail traffic.

Employees should be especially cautious with links from unknown senders and must never click suspicious links.

1.10 Passwords

Passwords protect access to personal data and must remain confidential.

Password rules:

- Minimum 8 characters
- At least one uppercase or lowercase letter
- At least one number
- At least one special character

Passwords must not be written on notes such as Post-its.

Different applications require different passwords.

Employees must never exchange passwords.

---

2. Operational Organization and IT Security

The best protection against security breaches is well-trained employees.

The company provides organizational and technical measures to support compliance with security requirements.

2.1 Clean Desk Policy

Only documents necessary for the current task may remain on desks or desktops.

Open files must be secured when leaving the workplace.

2.2 Leaving the Workplace

At the end of work:

- PCs must be shut down
- Documents must be removed from desks
- Windows and doors must be closed

2.3 Virus Protection

The company uses multilayer virus protection.

Unknown files or external storage devices must not be connected or opened.

In case of suspected malware infection:

- Stop working immediately
- Disconnect the device from power/network
- Inform IT or management

2.4 Visitors

Visitors may only enter office areas when accompanied by an employee.

Visitors are not granted access to internal IT systems.

2.5 Home Office

Home office work is permitted only according to employment contract regulations.

Company security standards must also be maintained at home.

Company network access must occur exclusively via VPN.

2.6 Security Measures

Employees may not bypass security mechanisms, including:

- Disabling password protection
- Disabling antivirus or firewall systems
- Using unauthorized storage media
- Running unauthorized software

2.7 Remote Maintenance

Employees acknowledge that the IT department may access systems remotely for support purposes.

Such access occurs in coordination with the employee.

2.8 Files and Paper Records

Paper documents must be stored properly.

Sensitive personnel files must be kept locked.

Unneeded records must be securely destroyed.

2.9 Violations

Gross negligence or intentional violations may result in disciplinary action.

2.10 Access to Server Rooms

Only authorized personnel may access server rooms.

Server rooms and cabinets remain locked.

2.11 Social Engineering

Personal data may only be disclosed to clearly authenticated individuals.

Suspicious instructions must always be verified through a second communication channel.

2.12 Data Breaches

In the event of a data breach, the Data Protection Officer and/or management must be informed immediately.

Employees may not act independently outside official instructions.

2.13 Rights of Data Subjects

Employees must immediately inform the Data Protection Officer if data subject rights are asserted.

These rights include:

- Right of access
- Right to rectification or deletion
- Right to restriction of processing
- Right to object
- Right to data portability
- Right to lodge complaints with supervisory authorities

---

3. Disruptions, Failures, and Security Incidents

Relevant contacts must be informed immediately in the event of:

- Security incidents
- Operational disruptions
- IT system failures

---

4. Data Storage / Backup and Recovery Concept

4.1 Principles of Data Storage

Data should generally not be stored locally on end devices.

Data must be stored on approved servers and network systems.

4.2 Data Backup

The company coordinates backup schedules and storage methods with administrators.

Backups must be created at least daily.

4.3 Rules for Administrators

Administrators must:

- Document storage locations
- Coordinate new storage structures with management
- Maintain backup and recovery concepts
- Conduct regular recovery tests

---

5. Deletion Concept

5.1 General

Personal data must generally be deleted when it is no longer required unless legal retention obligations apply.

Deletion means irreversible destruction or anonymization of data.

5.2 Deletion Periods

Personal data must be deleted if:

- It is no longer needed
- Consent has been withdrawn
- Processing is objected to without overriding legitimate grounds
- Data was processed unlawfully
- Legal obligations require deletion

Retention Obligations

According to the German Fiscal Code (AO)

Retention obligations apply particularly to:

- Accounting records
- Business correspondence
- Invoices
- Financial documents

According to the German Commercial Code (HGB)

Retention obligations also apply to:

- Commercial books
- Business letters
- Accounting documents

Retention Periods

- 10 years: accounting and financial documents

- 6 years: commercial and business correspondence

---

6. Consequences of Violations

In the event of misuse, the company may impose disciplinary measures including:

- Ordinary termination
- Immediate dismissal
- Civil claims for damages
- Criminal prosecution

---

7. Hierarchy of Rules

If provisions of this agreement conflict with other instructions or agreements, this agreement shall prevail.

---

8. Final Provisions

Changes to this agreement must generally be made in writing.

If individual provisions are invalid, the remainder of the agreement remains effective.

Schirm GmbH