



Information Technology (IT-)Governance

Diersch & Schröder Group
Status 2024

ENERGY

DS // WESER-PETROL

DS // MINERALÖL

DS // CARD+DRIVE

CARD+DRIVE
Polska

LANFER
ENERGIE

E M O V A
Energie. So einfach.

UTG
Unabhängige Tanklogistik GmbH

ENERGU

HAUER

WESER
TANKING

LEU.

CHEMICALS

ADDITIV
CHEMIE
LUERS

ESTICHEM^{AS}

ACF

LEVACO
CHEMICALS

Sparks

YOUNG BUSINESS

SCS

ELAPRO

ecopox

polytives

Lynatox



CONTENTS

PAGE	CHAPTER
05	Objectives of IT Governance
06	Responsibility
08	Use of IT Systems
11	Logging
11	Abuse Control
12	Attacks by Viruses, Hackers, and Similar Threats
13	Social Media
14	Procurement (Hardware and Software)
14	Cyber Insurance
14	Artificial Intelligence
14	Violations of IT Governance



Dear Readers,

The rapid evolution in our digitalized world not only leads to opportunities but also presents new challenges. In particular, the increasing complexity and the risk posed by cyber threats **demand a high level and security awareness**. The demanding regulatory requirements, in particular within the scope of KRITIS, highlight the necessity of protecting our digital resources.

With our IT Governance – which is binding for all executives and employees (hereinafter referred to as “the employees”) of Diersch & Schröder GmbH & Co. KG and its affiliated companies (hereinafter referred to as “DS Group”) – we are not only **requesting the responsible management of our IT infrastructures** but also sending a strong message regarding the challenges of our company's digital transformation.

Together, we contribute that the DS Group can operate safely and efficiently in this complex and regulated environment.

Your commitment to this IT Governance secures the digital future of our organization.

Bremen, September 1, 2024



Jan Christiansen

Chief Executive Officer
of the Diersch & Schröder Group



Objectives of IT Governance

With this IT Governance, we set a framework for efficient, secure and business-supportive IT practices. More detailed descriptions of specific IT topics shall be defined in separate guidelines.

Our IT Governance shall define how to use Information Technology (IT) in alignment with the strategic objectives of the DS Group.



● Understanding

We aim a shared understanding of the principles of our IT Governance to become "BETTER TOGETHER". *For example, understanding will be promoted through training sessions.*

● IT Security Standards

We strive to protect ourselves from viruses, trojan, and malware, and to defend external intrusions. *For example, by regularly updating antivirus programs and firewalls, as well as raising employee awareness of safe online practices.*

● Protection of Business-Secrets and Personal Data


We protect business data, confidential information and personal data. *For example, through the implementation of encryption measures for personal data and stringent access control policies.*

● Secure and Sustainable Operation of IT Infrastructure

We want to ensure a secure and sustainable operation for our business processes. *For example, by maintaining IT systems regularly to ensure their performance and implementing emergency plans for rapid recovery in case of failure.*

● Set up and use IT Infrastructure in accordance with applicable Laws

We comply with relevant legal regulations, particularly in the context of critical infrastructure. *For example, by implementing measures to adhere to data protection regulations, industry-specific standards, and other relevant laws.*



A fundamental prerequisite is the cooperation of all business units and employees within the DS Group to achieve these objectives.

2 Responsibility

2.1 The Parent Company and the Information Security Officer (ISO)

The Management of Diersch & Schröder GmbH & Co. KG and the Information Security Officer (ISO) are responsible for the content and oversight of the IT Governance. The ISO leads, monitors, and continuously improves information security within the DS Group. In the event of information security incidents, the ISO must be involved.

Diersch & Schröder GmbH & Co. KG ensures that employees receive trainings, instructions, and guidelines for handling IT systems, media, and data appropriately.

2.2 The Managing Directors of the Subsidiaries

The respective Management of each company within the DS Group (hereinafter referred to as "DS Unit") is responsible for implementing the IT Governance within the respective DS Unit. The IT Department with support of the ISO ensures the operation of the IT infrastructure and IT systems.

2.3 Employees

Every employee of the DS Group must adhere to the IT Governance regulations, actively contribute to the security of our IT infrastructure, and act responsibly when handling data, devices, and IT systems.



Use of IT Systems

IT systems provided by the DS Group and all the data contained are necessary tools for our daily work. The data contained within these systems is integral to them. Both the IT systems and data remain the property of the DS Group throughout their entire lifecycle.

If employees no longer use the IT systems (e.g., upon leaving the company), all components, including data, must be returned to the DS Group.

To ensure the IT systems function properly, they are regularly inspected and maintained. The DS Group also employs external service providers for this purpose. Employees are obliged to support the work of these experts. Planned maintenance will be announced in advance.

3.1 Private IT Systems

3.1.1 Use within the Corporate Network (LAN, WLAN)

The use of private IT systems, such as desktops, notebooks, or other systems or IT components, within the corporate network (e.g., by connecting to a network port or integrating into the WLAN) of the DS Group is not permitted.

3.1.2 Access to Corporate Data, Applications, and Services (Network)

Access to data and services of the corporate network (e.g., MS365 applications, Citrix, VPN) on private devices is only permitted for private mobile phones and tablets (e.g., iPads) that can be used within the BYOD (Bring Your Own Device) program (e.g., MS365). These devices must be secured using the deployed Mobile Device Management System in place (e.g., Intune).


3.2 Private Use of IT Systems

In general, private use of IT systems provided by DS Group is not allowed. Exceptions for the use of company phones and mobile devices are provided in the "Guideline for Communication Media" and in contractual agreements.

Private use of the company phone (internet, calls, apps, etc.) is still allowed outside working hours. However, it is not permitted to use company contact information (email address, phone number and any equivalents) for private purposes.

3.3 Business Emails

When using the business email the following points must be adhered to:

- 
- **Attachments**
Avoid attachments: Instead of sending attachments, files should be shared via a common storage location (e.g., OneDrive).
 - **External Emails**
External emails are marked as such. Despite all security measures, exercise special caution when opening attachments and links.
 - **Recipient Scope "Need to Know"**
Limit the use of "cc" or copies to the necessary minimum. Assess whether all recipients require or are authorized to receive the information.
 - **Absence**
For absences of one working day or more, set up an automatic reply for senders, including an estimated date of return.
 - **Chat vs. Email**
Avoid back-and-forth email exchanges as a question-answer thread. The chat function in MS Teams is often more effective for this purpose.
 - **Forwarding**
Automatic forwarding to email addresses outside the DS Group is prohibited. This also applies to forwarding to private email addresses of the user.
 - **Signature**
Automatic email footers (signatures) containing legal disclaimers must not be shortened, modified, or removed.

3.4 Passwords

The protection of passwords is the responsibility of the employees. The following must be observed:

- **Confidentiality:** Passwords must be kept confidential and must not be shared with others.
- **No Insecure Records:** Avoid writing passwords down on paper or storing them unencrypted on systems or media.
- **Suspicion of Compromise:** If a password is compromised or there is suspicion of compromise, it should be changed immediately.

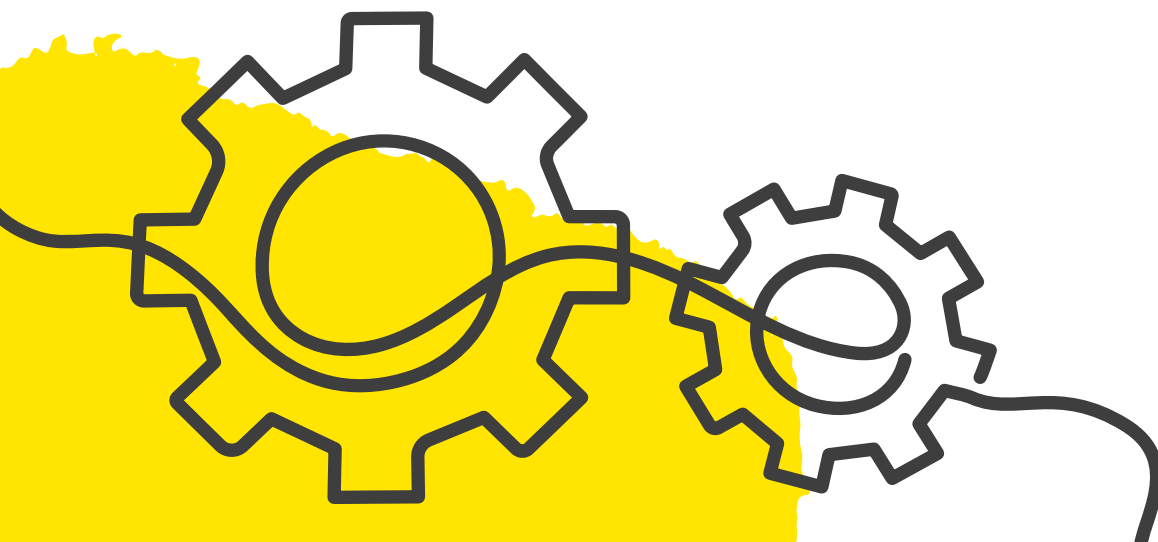
- **Strong Passwords:** Use strong passwords. If the IT system does not specify requirements, passwords should ideally contain uppercase letters, lowercase letters, numbers, and special characters. Passwords should be at least 8 characters long. More than 10 characters are recommended.
- **Passphrase:** Use a passphrase to create a complex password that is easier to remember.
- **Different Passwords:** Use different passwords for business and personal purposes.

All systems must be password-protected. Single Sign-On (SSO), such as authentication through a one-time system login, is preferred.

3.5 Software Usage and/or Installation

The introduction of software is based on necessity and may require a project initiation process. Test and demo versions require prior consultation and approval from the IT Department.

- **Data Protection Approval:** It is mandatory that every software is included in the Procedures and Software Directory and, if needed, in accordance to Data Protection Law approved by the Data Protection Officer (DPO).
- **Information Security:** The use of any type of application (SaaS, web applications, portals, apps, locally installed applications, etc.) must be coordinated with the IT Department, which will obtain any necessary approvals (e.g., from the ISO, DPO).
- **Licenses:** Privately licensed or unlicensed software (pirated copies) is strictly prohibited. Additionally, the download and storage of programs and files for non-business purposes on DS Group IT systems are not permitted.
- **Security Measures:** Software and data which are illegal or classified as critical to operations or security may be deleted without prior notice, potentially automatically through technical security measures.
- **File Storage:** Storing files on workstations or mobile devices must exclusively utilize synchronization with approved cloud providers (e.g., Microsoft OneDrive), ensuring continuous updates and security. Local, non-synchronized file storage is prohibited.



- **Software Installation:** Software installation is conducted by the IT Department only. Independent installation of software is prohibited.

These regulations apply equally to locally installed applications and SaaS (e.g., cloud/internet portals) applications.

3.6 Notebooks, Tablets, Smartphones and Mobile IT Systems

3.6.1 Use of Mobile IT Systems

Mobile IT systems such as notebooks, tablets, and smartphones pose potential threats for unauthorized access to DS Group information. Employees are not allowed to share their mobile devices with third parties.

When used externally, it is crucial to ensure that sensitive information is not compromised. It is recommended to process in particular sensitive data in locations not visible to third parties.

Data storage on mobile devices should only be executed for dedicated tasks, as local storage is not backed up. It is essential to ensure that all information is stored exclusively in approved locations. Encryption must be technically ensured, and data must meet synchronization requirements.

3.6.2 Central Management

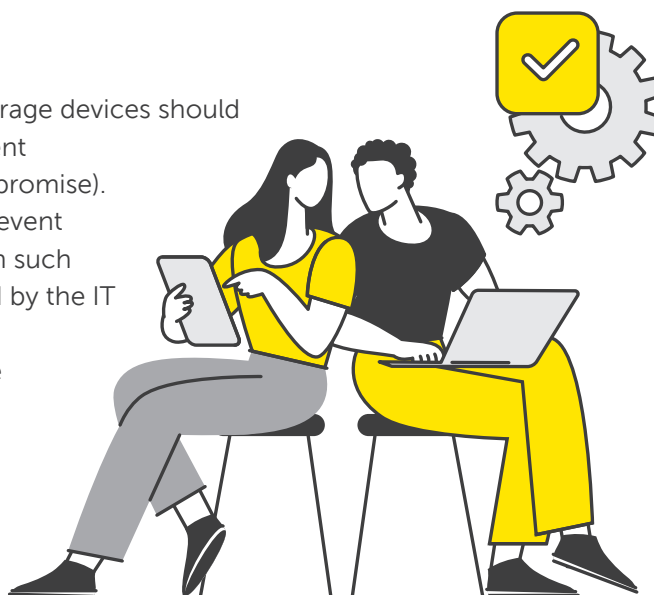
The management of mobile IT systems, including software installation, is handled via the Mobile Device Management (MDM) system. All mobile devices must be connected to MDM, and usage without connection to this system is not permitted.

3.6.3 Theft and Loss

Lost or stolen IT systems must be reported immediately to the IT Department. The IT Department will inform the ISO and the DPO. Delayed reporting may result in fines. In the case of theft, a report to the police is required. The IT Department will implement protective measures such as remote locking or data wiping.

3.6.4 Mobile Storage Devices

In general, the use of mobile storage devices should be avoided, as they always present a security risk (loss, defect, compromise). Precautions must be taken to prevent the loss of information stored on such devices. The guidelines provided by the IT Department must be followed. Unused storage devices must be disposed by the IT Department.



It is not allowed to connect found storage devices to the DS Group's IT systems. There is a risk that the device may contain malware or spyware. These devices should be handed over to the IT Department. The IT Department will inspect these devices and destroy them in case of harmful content.

3.7 Use of External Platforms (e.g., Cloud Services)

External platforms accessible via the internet may only be used when necessary for business operations and should be kept to a minimum. Common security guidelines such as password rules and two-factor authentication must be adhered to. Generally, platforms should be integrated with the Active Directory to enable global password policies.

- **Limited Use:** The use of external platforms should be restricted and the number of such platforms should be minimized.
- **Approved Platforms and Service Providers:** Approved platforms and service providers (e.g., MS365 environment) shall be preferred.
- **Ownership of Access Data:** Business data on external platforms remains the property of DS Group. This IT Governance shall apply appropriately.
- **Safety Standard:** It is only allowed to use platforms that meet current security standards. Verification is the responsibility of the IT Department.
- **Security Check:** Employees which use external platforms are required to regularly consult with the IT Department to check if the security status of the respective platform is still be valid.



3.8 Security Measures for Mobile Office

For "mobile work", agreements stipulated in the employment contract or similar documents are binding. The following must be observed when working remotely:



*Additionally, regularly check personal network devices at home, such as internet routers, for firmware updates.



For questions regarding the IT Governance, please contact the IT Department of Diersch & Schröder GmbH & Co. KG.
Email: ITGovernance@ds-bremen.de

4 Logging

The logging of IT activities not only monitors our systems but also ensures the legal compliance and security of our IT infrastructure.

Our logging is designed to provide comprehensive protection for sensitive data while adhering to the highest standards of data privacy and security.

Log data is not used for performance or behavioral monitoring of employees but is solely intended for identifying disruptions, outages, security incidents, and for optimization purposes.

5 Abuse Control

To prevent unauthorized access and illegal activities, specific measures for abuse control are implemented. Employees are encouraged to report suspicious activities to the IT Department immediately.

In the event of suspected abuse, the following measures will be taken:

- **Technical Prevention:** Automatic technical measures to prevent abuse of IT infrastructure will be implemented in coordination with the Information Security Officer (ISO).
- **Personal Review:** Detailed log reviews will only be conducted in cases of serious abuse suspicion, with mandatory involvement of the Compliance Officer.
- **Involvement of the Compliance Officer:** The Compliance Officer is an integral part of the review process in cases of significant abuse suspicion.
- **Deletion of Unconfirmed Suspicions:** Unconfirmed suspicions will lead to the immediate deletion of all reviewed data, without further action.
- **Immediate Action in Case of Imminent Danger:** The ISO will take immediate action to prevent harmful activities. Subject to specific conditions and in coordination with the Compliance Officer, law enforcement authorities will be involved.

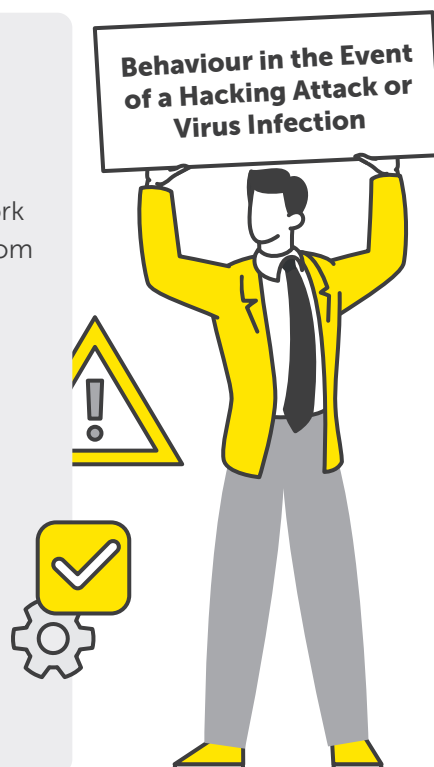
6 Attacks by Viruses, Hackers, and Similar Threats

All employees are required to report any incident or security breach to the IT Department immediately. The following should be observed:

6.1 Immediate Actions

In the event of suspected virus infection or a hacking attack, prompt immediate actions are crucial to minimize potential damage. Isolating the affected system will contain the spread of malware or hacking activities.

- **Disconnect Network Connection:**
Immediately disconnect from networks, especially corporate networks or sensitive personal networks. This can be done by deactivating WLAN or disconnecting network cables. If in doubt, disconnect the device from the power supply / switch off.
- **Report Security Incident:**
Report the suspicion of a virus infection or hacking attack immediately to the IT Department. Provide as many details as possible to facilitate a faster and more targeted response.
- **Activate Security Software and Scan:**
Perform an immediate system scan using installed security software (e.g., antivirus program, firewall) to detect and address potential threats.



6.2 Unchanged Damage Profile

The damage profile of an incident must not be altered. Preserving the original state of the incident not only facilitates resolution efforts but is often crucial for forensic analysis in case of damage. In the event that third parties are involved or if there are claimable damages, the integrity of the damage profile is essential for both legal proceedings and insurance purposes.

Exceptions to this rule apply only to immediate prevention and mitigation measures that can be taken without altering the damage profile.

6.3 No Direct Access to Infiltrated Systems

In the case of infiltrated systems, such as those affected by a hacking attack, no direct access to the compromised system is allowed, even by administrators. This measure is in place to protect the integrity of the data and to ensure a thorough analysis of the incident by IT security experts.

Social Media

The use of social media in a professional manner requires careful consideration to minimize potential security risks. Employees are required to adhere strictly to the following:

- **Separation of Professional and Personal Sphere:** Social networks such as Facebook, Instagram, LinkedIn, X (formerly Twitter), and similar platforms should be used exclusively for personal purposes. Any professional use must be done in collaboration with the Marketing Department.
- **Responsible Online Presence:** All online activities are public and can be viewed by the general public, including colleagues, clients, suppliers, and competitors.
- **Protection of Company Information:** It is not allowed to share internal company information, trade secrets, details about the company strategy, and the financial status of the DS Group. Personal data should not be shared without the consent of the individual concerned.
- **Respect for Copyrights:** Copyrights and intellectual property rights must be observed, as well as the right of personality in relation to images.
- **Clarification of Personal Opinions:** When expressing personal opinions, it is important to make it clear that these are personal views. Facts should be accurate, and employees should be aware that they may be perceived as representatives of the DS Group, even without explicit identification.
- **Permanent Consequences of Posts:** Information and posts on the internet are often permanently visible. Even if a post is deleted, its permanent storage cannot always be prevented.
- **Management of DS Group Profiles:** Employees managing profiles of the DS Group on social media are required to protect access using Two-Factor-Authentication (2FA) to prevent unauthorized access.

8 Procurement (Hardware and Software)

The IT Department is responsible for the procurement of hardware and software. All purchases of hardware and software must comply with established guidelines and processes. This ensures that the resources acquired are secure and compatible. A unified hardware catalogue exists for procurement, which specifies the types of hardware to be used by end-users (e.g., laptops, PCs, printers, monitors, etc.).

9 Cyber Insurance

Each DS Unit must secure itself against cyber incidents. The responsibility for ensuring appropriate insurance lies with the management of the respective DS Unit, in coordination with the Insurance Department of Diersch & Schröder GmbH & Co. KG.

10 Artificial Intelligence

- **Human Control:** AI Systems must be designed to ensure that employees retain decision-making authority over critical matters. Automated decisions should be subject to monitoring and confirmation by human operators.
- **Data Privacy:** AI Systems must ensure that personal data is protected and managed in compliance with Data Protection Laws, maintaining the privacy of employees, customers, and service providers. Sensitive data should be anonymized or pseudonymized if possible.
- **Implementation of new AI Systems:** When introducing new AI Systems, the following stakeholders must be involved: Compliance Officer, and if applicable, Data Protection Officer (DPO), Information Security Officer (ISO), IT Department, and Risk Management.

11 Violations of IT Governance

Compliance with this IT Governance will be subject to random checks. Any violations of this IT Governance will be reported to the management of the respective DS Unit, the Information Security Officer (ISO), the Compliance Officer, and the Human Resources Department. Such violations may result in disciplinary consequences.

ENERGY

Better together for **mobility, heat**
and electricity – that's what drives us.

CHEMICALS

Our **additives** lubricate industrial production
equipment and protect banana plants.

YOUNG BUSINESS

Start-ups help the DS Group to stay **young** and **innovative**.