Company employees, contractors, consultants and temporary staff (Trusted Parties) are required to handle information, whether physical, electronic or verbal, in accordance with Security Policy and the following rules and principles. You are expected to act ethically and according to local laws when representing the company.

1. If you are granted access to company’s systems, it is your responsibility to familiarise yourself with the security policies and comply with the relevant requirements of it. Your manager is responsible for identifying the requirements relevant to you and your area of responsibility.

2. Security at company premises

You should only use the main entrance, which is the door leading directly outside. You must keep good care of your key (card). Do not lend your key (card) to anyone or let others into company premises without valid access right. Do not wear your key (card) visible outside company premises. Guests must always be accompanied by a trusted party and not be allowed to walk freely on company premises.

Do not leave any windows or access-controlled doors, or doors generally unlocked.

3. Confidentiality

You must handle all company owned and governed information with discretion and care. This means You should not attempt to access or use information, systems, or networks you do not need for your assigned work. Do not store company information in cloud-, or other solutions unless the solution is approved by the company for the intended use.

When sharing information with others, make sure that there is a valid business reason for it. Before sharing information with non-employees verify that they have signed a non-disclosure or confidentiality agreement.

Avoid taking pictures, videos, recordings, and such on company premises. Only do so after careful consideration of the potential undesired impact if the contents is leaked.

4. Clean desk

Company has a clean desk policy. Securely dispose of unnecessary paper-and other hard copies. Store confidential information in locked drawers, cabinets, or the like to prevent unauthorised access. Clean whiteboards and remove papers from flipcharts after meetings.

5. Identity and access

You must safeguard your personal access rights and authentication information, such as passwords and pins, and not share them. Authentication information used to access company’s IT systems must not be re-used for non-employers governed services (e.g. social media or personal e-mail). You are allowed to store passwords related to your work only to a secure password storage solution approved by the company. You are solely and fully responsible for all actions performed by your company’s user account. Digital traces from your actions may be traced back to you as an individual, in accordance with GDPR and local legislation.

6. IT equipment and software

Never connect equipment to company managed equipment or to the internal network without appropriate approval. Company’s guests may use guest network. You may only install or download software approved by the company, and even then, only if you are authorized to do so.

To access company data on a mobile device (e.g. phone, tablet) the device must be enrolled to company corporate Mobile Device Management system. You are allowed to process company data on a mobile device only in apps managed by the company Mobile Device Management system.

Software and equipment provided by the company are company’s property and should be handled with care and not lent to others (including family members). Same care must be used with mobile devices containing company data. You must log-off or lock your computer and mobile device whenever you leave it.

7. Handling company information and equipment outside company premises

You must protect company information and equipment (e.g. mobile devices, laptops, USB sticks and such) against theft and unauthorised access outside company premises. You can achieve this by e.g. constantly supervising equipment and documents containing company information, carrying them as hand luggage or storing them in locked rooms. Also, keep conversations private, use privacy filter on your computer screen and show general vigilance to your surroundings.

Before going on a company business trip, familiarise yourself with the travel security guidelines.

8.Use of e-mail and Internet

You must minimise private use of Internet and e-mail on company equipment. Do not use company accounts or equipment to deliberately access sites with inappropriate, unethical or illegal content.

9. Security monitoring and logging

There is security monitoring and logging of company IT systems. However, company respects the privacy of the individual, and special situations in which company may need to access a user’s email account or other information created and stored by the user will be handled in accordance with local laws and regulations.

10. Report security incidents

Security incidents or suspected security incidents, e.g. unauthorised access to system or information theft, must be reported promptly to head of the company. If you lose company equipment, contact head of the company immediately. If any items stated in this document are unclear to you, contact your manager for more information.