TP2B THE PLACE TO BE

ATEA

INFORMATION SECURITY RISK MANAGEMENT: POLICIES FOR EMPLOYEES

Version 1.0 - published August 2019

LETTER FROM THE CEO

At Atea, our mission is to “Build the Future with IT”.

We believe that information technology, combined with knowledge and creativity, can improve productivity and living standards across society. We support companies and public sector organizations to build digital solutions which enable them to accomplish more, with greater efficiency and less resource consumption.

At the same time, we understand the risks inherent in technologies which store and process ever more information. As organizations handle more data and automate processes through their IT systems and networks, they face greater threats from data theft, identity fraud, and operational disruption through cyberattacks. A data breach may also result in a person’s data being accessed without their consent, and misused to harm that person and violate their right to privacy.

Atea is the leading provider of information technology in the Nordic and Baltic regions, and has a special responsibility to ensure that its operations conform to strict standards of information security. Atea designs, implements and operates IT infrastructure solutions for the largest and most vital organizations in our regions. Most of our sales are to national and local government agencies, including highly sensitive customers such as the military and police. We also provide mission-critical IT solutions to the biggest corporations in our regions.

This document is a guide for managing information security risks at Atea. It provides an overview of key security risks, data protection policies, and governance procedures which impact everyone in our company. Employees who have special responsibilities regarding IT operations and systems administration will be required to take separate, more extensive examinations on information security and data protection policies, as their function requires.

The document is broken into four sections, with highlights summarized at the end of each section. The four sections are detailed, as this is a complex and business-critical topic. It is particularly important that employees remember the “highlights” at the end of each section and are able to reference the remainder of the document when necessary.

The contents of this document are required knowledge for all Atea employees. To ensure that all Atea employees have understood the content of this document, ten questions relating to information security have been added to the Code of Conduct examination, a test which is mandatory for all Atea employees. An online training course is available for employees to study Atea’s information security policy and prepare for the Code of Conduct examination.

Atea is a large organization spread across seven countries and nearly 90 offices. A Chief Information Security Officer has been appointed for the Group and for each country to support the

Steinar Sønsteby
CEO

implementation of information security policy throughout the Atea organization.

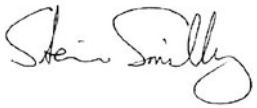
If you have questions or concerns regarding information security at Atea, we ask that you address your issues as follows:

- If you are concerned that your PC may be infected by malware or have general questions regarding IT security, please contact the Atea Servicedesk
- To report a suspicious email, fraud attempt or any other event which might represent an information security risk for Atea, please contact the Atea Servicedesk
- To report a suspected breach (unauthorized disclosure) of personal or business data from information systems and documents, please contact the Chief Information Security Officer of the country in which you work. Alternatively, you may send a mail directly to infosec@atea.com.

If you wish to speak directly with the Chief Information Security Officer (CISO) of the Atea group or the CISO of your country or shared service unit, their names can be on the Atea compliance website: atea.com/trust. Any mail sent to infosec@atea.com will be directly forwarded to the Chief Information Security Officer of the Atea group.

We are happy to receive your questions and feedback, and promise that there will be no retaliation for any concerns which are reported. However, if you prefer to report a concern anonymously, you can also submit a report to the Whistleblower Hotline. A link to the Whistleblower hotline can be found on the Atea compliance website: atea.com/trust. Concerns reported to the Whistleblower hotline are sent to an independent law firm, who will summarize and report your concern to the appropriate level of the Atea organization.

Maintaining strict standards of information security is essential to our business at Atea, and to our ability to work with customers and partners on the most important IT challenges in our region. Thank you for following Atea's information security policies, and for making Atea "The Place to Be".



Highlights:

It is essential for Atea that all employees maintain strict standards of information security.

A Chief Information Security Officer has been appointed for the Group and for each country to support the implementation of information security policy throughout Atea. Names of the Chief Information Security Officers can be found on the Atea compliance website: atea.com/trust.

If you have questions or concerns regarding information security at Atea, we ask that you address these as follows:

- If you are concerned that your PC may be infected by malware or have general questions regarding IT security, please contact the Atea Servicedesk
- To report a suspicious email, fraud attempt or any other event which might represent an information security risk for Atea, please contact the Atea Servicedesk
- To report a suspected breach (unauthorized disclosure) of personal or business data from information systems and documents, please contact the Chief Information Security Officer of the country in which you work.
- Alternatively, you may send a mail to infosec@atea.com, which will be forwarded directly to the Chief Information Security Officer of the Atea Group

Content

1. INFORMATION SECURITY – OVERVIEW AND RISK MANAGEMENT

Information is essential to the functioning of any organization. An information security management system (ISMS) is the set of policies, procedures, tools, and activities which an organization uses to protect its information assets from unauthorized access and misuse.

Creating an ISMS requires that an organization identify the information assets which it holds. This includes all data which the organization handles regardless of form: digitally, on paper, or verbally. At Atea, this information may be for internal use, or may be external data which Atea manages and processes as a service for its customers.

The purpose of an information security management system is to protect and preserve the confidentiality, integrity, and availability of information assets.

- **Confidentiality** means that information is only made available to authorized persons.
- **Integrity** means that information is maintained so that it is complete and accurate.
- **Availability** means that authorized users can access and use data when needed.

To achieve these objectives, an organization should conduct a risk assessment to identify how its information assets are exposed to potential information security threats. It can then design an information security management system which can manage and control these risks in an effective manner, without unnecessary cost or lost productivity.

Risk assessment at Atea

The following information security risks have been identified as the highest priority for Atea's business:

1. **Physical loss:**
   Information assets are stored on physical devices, which can be lost, stolen or damaged. Access control, encryption and data backup are essential to limit the potential risks to physical assets, such as PC's, mobile phones, servers and storage. Data centers are particularly vulnerable, and must be protected from environmental hazards including temperature and fire.

2. **Identity fraud:**
   Atea is continually exposed to fraud attempts, by attackers who use false identities or deception to take advantage of an employee's trust. The objective of the fraud attempt is usually to steal from Atea or to gain unauthorized access to Atea's systems and networks.

   One type of identity fraud against Atea is the use of a false or stolen customer account data to order IT equipment, particularly through the Atea Eshop. In addition to access controls on its Eshop, Atea has business routines to screen new customer accounts and identify unusual customer activity on existing accounts to reduce the risk of fraudulent customer transactions.

   Another very common form of identity fraud ("phishing") occurs when an attacker contacts an Atea employee directly, most frequently through an email communication. The email appears to be from a trusted source, often by using a false identity such as that of another Atea employee, a business associate, or a vendor such as a technology firm or bank. The email attempts to deceive Atea employee into a response, such as transferring money, entering login/password data or other sensitive information, or clicking a link or attachment which downloads malicious software ("malware") onto the user's PC or mobile.

   The mail, attachment or link will appear to be innocent – for example, will be disguised as a mail from a colleague, an offer/invoice from a vendor or as a notification from a cloud account such as OneDrive. For this reason, Atea employees must be extremely alert to the potential of fraud in any email or other communication, even if the communication appears to be from a trusted source.

   Atea employees should never open links or attachments from their devices if they have doubts about the legitimacy of an email or communication. If an Atea employee is

uncertain about the legitimacy of an email, or if they have accidentally responded to a possible fraud attempt through opening a suspicious link or attachment, they should immediately contact the Atea Servicedesk to report their concern.

While email is the most common method for "phishing" attacks related to work, Atea employees should also be alert to other forms of fraudulent communications, including telephone inquiries or social media invitations.

3. Theft of business secrets:

If unauthorized persons gain access to Atea's information systems, they may attempt to steal proprietary information which is sensitive for Atea's business. This may include secretive business information such as customer or supplier data, contracts, and commercial terms. This may also include intellectual property, such as business concepts, product or service designs, and internally-developed software, methodologies and tools.

Employees with access to key systems may also attempt to steal business secrets from Atea, especially if they have plans to leave the company. To reduce risk, access to information must only be granted to employees on a "need to know" basis. System access should continually be screened to ensure that the "need to know" principle is maintained, and that a user's access rights are terminated when no longer needed.

4. Disruption of business operations:

Atea's business operations are dependent on its IT systems. If access controls are breached or if systems are misused, information which is private to employees or business associates can potentially be leaked. Information which is necessary for Atea to conduct business could be tampered with or deleted. Finally, business transactions can be entered or approved by unauthorized persons, in breach of Atea's management controls. All of these events are disruptive to Atea's business operations.

Atea is also at risk of a disruption to its operations through a sophisticated hacking attack which shuts down key IT systems or networks. Systems may be infected with malware that prevents users from accessing critical functions or from reading data files unless a ransom is paid ("ransomware"). Networks or servers may be flooded with traffic or requests, so that they are no longer able to handle legitimate transactions ("denial-of-service" attack). These attacks may target either Atea or the customers which Atea manages from its data center.

5. Contractual damages:

Atea has confidentiality agreements with many customers, vendors and business partners. Atea also has service level agreements and data processing agreements with customers who use Atea's IT services and support.

An IT security incident at Atea can lead to Atea violating its confidentiality, service level and data processing agreements with customers and other business partners. This may result in lawsuits against Atea to compensate for damages due to violation of the contracts. In addition to direct damages, an IT security incident can cause lasting harm to Atea's business relations with customers and partners.

Even in situations where Atea does not have a specific contract, Atea can face legal claims from companies or individuals in the event that their data is stolen or misused if Atea did not demonstrate due care when handling the data.

6. Regulatory penalties:

As a listed company on the Oslo Stock Exchange, Atea must follow strict legal requirements when handling data which is not known in the market and which may have an impact on its share price ("price-sensitive information"). This may include information on major new contracts or financial results which have not yet been reported to the public.

Atea must manage price-sensitive information confidentially to ensure that this information is not distributed outside of a limited number of registered insiders on a “need to know” basis. Employees holding price-sensitive information must be registered by the company, and are subject to special nondisclosure requirements and restrictions on trading in the shares of Atea. Violation of these legal requirements is subject to prosecution and regulatory penalties under the Norwegian Securities Trading Act.

Atea is also subject to possible regulatory penalties in the event of a data breach involving personal data, under the General Data Protection Regulation (GDPR) of the European Union. As the requirements of the GDPR are quite extensive, this topic will be covered separately in the next section of this document on data privacy.

Highlights:

All employees must be very careful in their handling of information and IT systems to prevent a security breach.

IT equipment can be lost, stolen or damaged. Access control, encryption and data backup are therefore essential to limit the potential information security risks.

Atea is continually exposed to fraud attempts, by attackers who use false identities or deception to take advantage of an employee’s trust. Be aware that any email or other communication that you receive may be a fraud attempt, even if it appears to be from a legitimate source (including a mail from an Atea executive, a customer, a technology vendor, or a social media account).

Be on guard for any unusual communication or activity that you are may see. If you are suspicious that you are being targeted for fraud through an email or other message, please contact the Atea Servicedesk with your concern. Do not respond to any suspicious communication – for example, by opening email attachments and external links, or by processing orders and payments.

Access to information must only be granted to employees on a “need to know” basis to reduce the risk of information theft or misuse. System access should continually be screened to ensure that a user’s access rights are terminated when no longer needed.

An information security incident may result in serious harm to Atea through disruption of its business operations, violation of Atea’s contractual obligations toward customers and business partners, regulatory penalties, and damage to Atea’s reputation and business relations.

2. DATA PRIVACY – OVERVIEW AND RISK MANAGEMENT

Data privacy involves a person's control over their own data – specifically, their ability to determine when and how their own data is collected, shared and used. Personal data is defined as any information in any form which can be referenced to a specific and identifiable person.

Data privacy is dependent on information security, i.e. how data is protected from unauthorized access and misuse. However, data privacy also extends beyond information security into the protection of an individual's rights to their own data. Specifically - how does an organization provide each person with the ability to control the use of their personal data when the organization gathers and processes information regarding that person.

At Atea, we believe that data privacy is a fundamental human right, and we are committed to handling personal data in a manner which fully respects this right. Atea is subject to strict legal requirements when handling personal data under the General Data Protection Regulation (GDPR) of the European Union.

The GDPR's requirements as they apply to Atea can be summarized as follows:

Requirements when gathering personal data

Atea can only process (e.g., gather, store and use) personal data when it has a legitimate business interest, and when the relevant person has granted consent or been notified that their personal data is being processed. The details of this notification or consent are described in the next section of this document.

Right of persons to control their personal data

Atea must comply with an individual's request to control the use of their personal data, in accordance with their rights to data privacy under the GDPR. Under the GDPR, individuals have the right to access their own personal data which is held by Atea. Individuals also have the right to rectify errors in their personal data, to have their personal data deleted, or to restrict the processing and use of their personal data.

Documentation of processing activities

Atea must document the extent of its data processing activities regarding personal data. This should include a description of what types of personal information are being processed and for which categories of persons. This should also include a description of which technical and organizational measures have been taken to prevent and minimize the impact of a data breach in Atea's data processing activities ("privacy by design").

Data processing agreements with customers / vendors

When Atea provides data processing services to customers (e.g., when Atea manages data infrastructure and applications for customers, either at the client's site or from its own data centers), Atea must also have a valid data processing agreement in place with the customer which is compliant with GDPR requirements.
Similarly, when Atea processes personal data through a subcontractor or vendor (e.g., when it uses software applications operated in a vendor's data center, such as cloud services), Atea must have a valid GDPR-compliant data processing agreement with the company that is managing the application and processing personal data on Atea's behalf. Information which is processed outside of the EU/EEA must be in a country or under a framework which the public authorities have approved as having adequate safeguards for data protection.

Requirements in the event of a data breach

In the event of a personal data breach which may result in the risk of harm to an individual, Atea must notify the supervisory authority of the country in which the breach occurred within 72 hours of becoming aware of the breach. The notification must describe the nature of the breach, a summary of the data subjects and records concerned, the likely consequences of the breach, and the measures being taken.

Individuals whose personal data has been breached must also be notified directly if there is a high risk of harm to that person. A public communication may be sufficient if individual notification is not achievable.

Under the GDPR, the supervisory authority of each nation can impose high penalties on a company in the event of a GDPR violation. The amount of penalty is based on the nature of the violation, the extent of harm to data privacy rights, and the measures the company has taken to prevent and address the violation. The maximum penalty in the event of a GDPR violation is 4% of annual global revenue or 20 million Euro, whichever is higher.

Based on the GDPR requirements, it is critical that Atea documents all routines involving personal data, and identifies all internal applications and contracts which involve the processing of personal data. This information must be available to the Chief Information Security Officer of each country, to confirm that appropriate measures are in place to protect data privacy. The Chief Information Security Officer of each country and of the Group can be found on the Atea Compliance website.

Highlights:

Data privacy involves a person's control over their own data – specifically, their ability to determine when and how their own data is collected, shared and used. Personal data is defined as any information in any form which can be referenced to a specific and identifiable person.

Atea is subject to strict legal requirements when handling personal data under the General Data Protection Regulation (GDPR) of the European Union.

Under the GDPR:

Atea can only process (e.g., gather, store and use) personal data when it has a legitimate business interest, and when the relevant person has granted consent or been notified that their personal data is being processed.

Atea must comply with an individual's request to control the use of their personal data, in accordance with their rights to data privacy under the GDPR.

Atea must document the extent of its data processing activities regarding personal data, including which measures have been taken to prevent and minimize the impact of a data breach. This requires that Atea documents all routines involving personal data, and all internal applications and contracts which involve the processing of personal data.

Atea must have a valid data processing agreement in place with all customers for which it provides data processing services (e.g., managing data infrastructure and applications, either at the client's site or from its own data centers).

Atea must also have a valid data processing agreement any subcontractor or vendor that is processing personal data on Atea's behalf (e.g., providing software applications and data storage operated in a vendor's data center, such as cloud services).

In the event of a personal data breach which may result in the risk of harm to an individual, Atea must notify the supervisory authority of the country in which the breach occurred within 72 hours of becoming aware of the breach.

3. DATA PROTECTION POLICIES AT ATEA

Atea employees must follow the company's data protection policies at all times when collecting, handling and distributing data. All Atea managers are responsible for ensuring that business processes within their area of responsibility follow Atea's data protection policies, and that their employees are working according to these business processes.

All Atea managers are assigned to a Data Protection Administrator who is responsible for a specific business function in their country (or shared services unit). The role of the Data Protection Administrator is to review that all business processes within their business function are compliant with Atea's data protection policies. These functions include: Sales/Marketing, HR, Finance, Consulting services, AMS, Logistics, and IT.

The Data Protection Administrator for each business function reports into the Chief Information Security Officer of the country (or shared service unit). The Chief Information Security Officer of each country has overall responsibility for the implementation of data protection policies within that country, and reports to the Chief Information Security officer of the Group.

Contact information for all key members of the Information Security organization in your country can be found on the Atea compliance website: atea.com/trust. A summary of the Information Security organization is also provided in the appendix to this document.

Atea's data protection policies cover:

- System registration
- Data classification
- Personal data management
- Customer agreements

An overview of data protection policies follows:

System registration

Before Atea employees start a process to collect, handle or distribute information, they must confirm that all information systems which will store or process the information are registered and authorized by the Chief Information Security Officer of the country. This includes any cloud services which are purchased through a subscription and managed outside of Atea.

The Chief Information Security Officer will conduct an analysis of the IT security and data privacy standards of an information system before registering the system to be authorized for use at Atea. The analysis is based on a checklist of IT security and data protection standards at Atea, and is completed together with the Chief Information Security Officer of the Atea Group.

The Chief Information Security Officer will also consider the type and sensitivity of data to be stored in the system when analyzing whether the system meets Atea's information security requirements. As part of the analysis, the Chief Information Security Officer will also approve a policy for deleting personal data in the system when it is no longer needed by Atea (a "data minimization" policy).

If the information system is externally managed and contains personal information – for example, a cloud-based HR system – Atea must have a signed data processing agreement (DPA) in place with the service provider to comply with the GDPR. A standard DPA for use with a cloud service provider is available on the Global Information Security webpage of your country's intranet. The Chief Information Security Officer in each country can answer questions regarding the DPA and can support the process of obtaining a signed DPA from the service provider.

Atea employees cannot store or process company data in "shadow IT" systems which are not registered by the Chief Information Security Officer of their country. Atea employees cannot make significant changes to systems or processes for handling data, without informing the Chief Information Security Officer so that a new evaluation of IT security can be made.

Once a system is authorized for use within Atea, a System Owner will be assigned to the system. The System Owner will be responsible for ensuring that the system is used according to Atea's data protection policies. In particular, the System

Owner is responsible for ensuring that access rights to the information system are limited to those with a "need to know", and are terminated as soon as they are no longer required. The System Owner is also responsible for ensuring that personal data stored in the system is erased when it is no longer needed by Atea, in accordance with the data minimization policy agreed when the system is approved for use.

Data classification

When a system is authorized for use at Atea, the type and sensitivity of data stored in the system will be documented to ensure that appropriate policies for data protection are maintained.

There are many cases however when Atea employees will handle and distribute information outside of an authorized IT system. This includes information handled through printed documents, through email communication or through sharing a file (i.e. a Microsoft Word/Excel/Powerpoint file).

To ensure that information held outside of an authorized IT system is managed with an appropriate level of information security, Atea employees must specifically mark any file, document or email which contains information according to its sensitivity so that this is understood by the recipient of the information. This marking must be in accordance with Atea's standards for data classification.

Atea's data classification standards consist of five levels, which rank the information stored in the email or file from least to most sensitive. The classification standards are directly built into Atea's versions of Microsoft Outlook and Word/Excel/Powerpoint. Atea employees can automatically mark an email, document or file with a correct data classification marking through selecting a button in the header of these software programs.

The five levels are as follows:

1. Non-business: Private email conversations and documents which are not related to Atea

2. Public: Information related to Atea which can be distributed publicly

3. Internal: Information which can be freely distributed internally at Atea or with Atea business units and contracted 3rd party suppliers. Not intended for distribution outside of Atea or contracted parties.

4. Confidential: Information which should be held private to the recipient, and must not be shared without the approval of the information owner. This includes personal data, which should be separately marked. A marking for personal data can be added through a drop-down menu under the Confidential button.

5. Strictly confidential: Information which would have significant negative consequences for Atea if disclosed without authorization. Should be stored in encrypted format and must not be shared without the approval of the information owner. Includes the following:

- Sensitive personal data: Under the GDPR, specific categories of personal data must be treated with extra security precautions. This includes information related to: ethnic origin, political opinions, religion, trade union membership, and genetic or biometric data. Sensitive personal data should be separately marked. This marking can be added through a drop-down menu under the Strictly confidential button.

- Sensitive business information: This includes business information such as key customer or supplier data, contracts, and commercial terms. It also includes information which is covered under a nondisclosure or confidentiality agreement with a customer or business partner. Finally, this may include highly sensitive intellectual property, such as business concepts and internally-developed software, methodologies and tools.

- Price-sensitive information: Price-sensitive information is a specific type of confidential information which may impact Atea's share price. This would include significant financial data which has not yet been reported, or the status of confidential negotiations relating to a very large customer contract or commercial agreement.

  The Group CFO of Atea must be immediately notified of all employees holding price-sensitive information. These employees will be registered in the Computershare Insider Management System (CIMS) used by Atea. Further information on compliance procedures for price-sensitive information can be found in the Code of Conduct.

A full description of Atea's data classification standards, and procedures for marking and encrypting documents and email communications

can be found on the on the Global Information Security webpage of your country's intranet.

Personal data management

Under the GDPR, Atea has special legal obligations when handling personal data – information which can be referenced to a specific and identifiable person. These legal obligations require Atea to document that it has taken sufficient technical and organizational measures to comply with the GDPR. This process documentation must be made available to the public authorities if requested.

Before Atea can collect personal data, the business process through which personal data is to be handled must be fully documented and reviewed by the Chief Information Security Officer. The Data Protection Administrator of each function is responsible for ensuring that all processes for handling personal data within their function are documented and up-to-date in accordance with GDPR.

The documentation must demonstrate that Atea has taken sufficient technical and organizational measures to comply with an individual's rights to their personal data, to prevent and minimize the impact of a data breach, and to respond lawfully in the event of a personal data breach. Processes for collecting personal data must also include a procedure for data minimization, i.e. deleting personal data when it is no longer needed by Atea.

When collecting personal data, Atea must notify an individual or obtain their consent that their personal data is being collected and used. When notifying or obtaining consent from an individual, Atea must communicate the following information according to the GDPR:

1. Categories of personal data being collected and processed
2. Purpose and legal basis of the data processing
3. Recipients of the personal data, or categories of recipients
4. Period of time that the data will be used, or the criteria that determines this period
5. Rights of the individual to their personal data -- including the right to withdraw consent and the rights of access, erasure and rectification
6. Right of the individual to complain to a supervisory authority.
7. If applicable, notification that the data will be transferred to a separate country, and a confirmation that any processing of data in a separate country will be in accordance with GDPR provisions on adequacy of data protection
8. If sensitive personal data is collected, Atea must request and receive explicit consent from the individual whose data is processed.

A standard privacy notice for collecting personal information is available on the Global Information Security webpage of your country's intranet.

Atea has special obligations under the GDPR in the event of a data breach involving personal information. A data breach is an information security incident which results in unauthorized persons gaining access to data or which results in the unlawful or accidental loss of data.

In the event of a data breach, Atea employees should immediately notify the Chief Information Security Officer of their country or shared service unit. The Chief Information Security Officer will investigate the data breach together with Atea's information security organization, and will take remedial action as necessary to report and mitigate any damage caused by the data breach.

If the data breach involves personal information and results in the risk of harm to an individual, Atea must notify the supervisory authorities of the country in which the breach occurred within 72 hours of becoming aware of the breach. The notification must describe the nature of the breach, a summary of the data subjects and records concerned, the likely consequences of the breach, and the measures being taken.

Individuals whose personal information has been breached must also be notified directly if there is a high risk of harm to that person. A public communication may be sufficient if individual notification is not achievable.

Customer agreements

Atea manages data infrastructure and applications for many customers, either at the client's site or from its own data centers. In these cases, Atea is contractually responsible for processing the customer's data, and has a legal obligation under the GDPR to ensure it will adequately safeguard the data privacy rights of any individuals whose personal information is included in the customer's data.

In order to comply with the GDPR, Atea must have a data processing agreement (DPA) in place with its customers when managing a customer's data infrastructure and applications. The data processing agreement must document the scope, nature and duration of data processing activities undertaken by Atea on the instructions of the customer.

This documentation must also include a summary of which types of personal information Atea will process on behalf of the customer and which categories of persons will have their personal information processed.

The DPA must include the following confirmation from Atea, in accordance with the GDPR:

1. Atea processes personal data only on documented instructions from its customer, and will comply with data protection laws
2. Atea employees who process personal data for the customer have committed themselves to confidentiality. Atea will not appoint subcontractors to process personal data for the customer without the customer's authorization.
3. Atea has taken sufficient technical and organizational measures to ensure a level of security agreed with the customer as appropriate to the risk of the data being processed.
4. Atea has taken sufficient measures to fulfill its legal obligations toward the rights of persons to control processing of their data, as described under the GDPR
5. Atea will provide the customer with any information necessary to demonstrate its compliance with data privacy obligations under the GDPR and participate in a compliance audit by the customer if requested
6. Atea will inform the customer of any breach of personal data without undue delay
7. Atea will delete or return all personal data to the customer at the end of the service agreement

If Atea uses external subcontractors to meet its data processing obligations to the customer (e.g., third party cloud services, consultants or infrastructure providers), Atea must have a separate DPA in place with these subcontractors, in which the subcontractor provides a similar confirmation to the statements written above.

Atea has a standard DPA which is recommended for use with all customers and subcontractors. The DPA is available on the Global Information Security webpage of your country's intranet. The Chief Information Security Officer in each country can answer questions regarding the DPA and can support the process of obtaining a signed DPA from the customer or subcontractor.

In the event of a personal data breach involving a customer's data, Atea must notify the customer without delay upon becoming aware of the data breach. Atea must then cooperate with its customer and take reasonable steps to ensure that the customer can meet its obligations to report the data breach as required by GDPR, and can take remedial action to mitigate the damage caused by the breach.

Highlights:

System Registration

All IT systems in use at Atea must be registered with the Chief Information Security Officer of the country or business unit where the system is in use. This includes cloud services which are purchased through a subscription and managed outside of Atea.

The Chief Information Security Officer will review the IT system to confirm that it meets Atea's IT security standards before approving the system for use. Once a system is registered, a System Owner will be appointed. The System Owner's role is to ensure the system is used according to Atea's data protection policies, with particular focus on managing access rights.

Data Classification

To ensure that information held outside of an authorized IT system is managed with an appropriate level of information security, Atea employees must specifically mark any file, document or email which contains information according to its sensitivity so that this is understood by all recipients. The marking must be in accordance with Atea's standards for data classification.

All routines for handling personal data must also be documented and reviewed by the Chief Information Security Officer. Every Atea manager is assigned to a Data Protection Administrator who is responsible for a specific business function in their country (or shared services unit). The role of the Data Protection Administrator is to review that all business processes within their business function are compliant with Atea's data protection policies, in accordance with GDPR.

Personal data management

When collecting personal data, Atea must notify an individual or obtain their consent that their personal data is being collected and used, in accordance with GDPR. GDPR has numerous information requirements relating to the content of the notification (see main text).

A data breach is an information security incident which results in unauthorized persons gaining access to data or which results in the unlawful or accidental loss of data. Atea has special obligations under the GDPR in the event of a data breach involving personal information.

In the event of a suspected data breach, Atea employees should immediately notify the Chief Information Security Officer of their country or shared service unit. Alternatively, a mail can be sent to infosec@atea.com, which will be forwarded directly to the Chief Information Security Officer of the Atea Group.

Atea must have a data processing agreement (DPA) in place with its customers when managing a customer's data infrastructure and applications, in accordance with the GDPR. Atea must also have a DPA in place with its subcontractors or vendors which process data for or on behalf of Atea. GDPR has numerous information requirements relating to the content of the DPA (see main text).

4. IT INFRASTRUCTURE SECURITY – REQUIRED PRACTICES FOR ALL EMPLOYEES

Atea's IT infrastructure consists of all hardware, software, and network components that support the delivery of business systems and IT-enabled processes to users. Data protection at Atea is dependent on all employees using Atea's IT infrastructure assets in a responsible manner.

The following policies relate to all employees at Atea as users of Atea's IT infrastructure, and cover device security, system access, file storage, network security, communications and physical security. In addition, employees with responsibility for managing Atea's IT operations are required to take separate, more extensive training on IT security corresponding to their function.

Device security:
Atea employees must take security precautions with their work devices such as PCs, tablets and smartphones. These devices are prone to theft, malware and unauthorized use. Atea PCs, tablets and smartphones should always be watched or stored in a secure location. When not in use, these devices should be locked with PIN/password protection or shut off.

All Atea PCs, tablets and smartphones should have encryption solutions installed to prevent unauthorized access to the hard drive. Atea Windows PCs are activated with the Bitlocker encryption solution. For Apple Mac models, there is a built-in function to encrypt the hard drive which must be activated with use. All iPhone and iPad devices are preinstalled with encryption. Encryption must be manually enabled on Android mobiles and tablets. Encryption should also be activated on removable memory such as USB drives, which can easily be lost. Employees seeking support for encrypting their work devices can contact the Atea Servicedesk.

Atea employees should not download software to their PCs that is not sourced from Atea's IT department. Atea's IT department offers a range of software applications through its Accelerator portal. These applications are regularly updated to maintain the correct level of security. If an Atea employee needs to download external software to their PC which is not from the Accelerator portal, they should first get approval from their manager and from their local IT organization.

Atea PCs are preinstalled with antimalware and firewall applications. If you have any doubt about your antimalware protection, contact the Atea Servicedesk. If you receive an antimalware program alert or if your computer acts abnormally, this may be a sign that your computer has been compromised. Signs of malware on a PC may include frequent freezing or unusually slow processing, or operations which take place without initiation, including popups or other changes on the screen.

If you suspect that your PC has been compromised, first discontinue all work on the computer and disconnect it from the network. Then contact the Atea Servicedesk, and provide information on what symptoms have created suspicion that the PC was attacked with malware, and what events may have led to the PC being compromised.

Any work devices which will be taken out of use must be cleared of all data before they are sent from the Atea office for service, recycling, or reuse. This should be done in accordance with the IT procedures implemented in each country. These procedures can be found on the Global Information Security webpage of your country's intranet.

System access:
Atea employees should only be granted access to systems when required for their work. Access rights to systems must continually be screened to ensure that this policy is maintained, and that access is terminated as soon as it is no longer required. If an Atea employee has access to systems which they no longer need, they should contact the System Owner immediately to terminate their access rights.

When system access rights are granted to an Atea employee, the user name and temporary password must be distributed separately. The

temporary password must be immediately changed after the first login, and should not be written down or shared with anyone. Employees must not lend out access rights to other users.

File storage:
All Atea employees are responsible for ensuring that their work files (e.g., MS Word/Excel/Powerpoint files) are securely managed. All types of files should be stored on Atea internal shared file servers, OneDrive accounts, or the Sharepoint environment. No other external storage sites, including Dropbox or Google Drive, may be used to store Atea files without explicit permission from the country's IT department, as Atea cannot guarantee the security of these storage sites. Atea employees should not store company information on the hard drives of their local devices, as this information is not automatically backed up and is therefore at risk of data loss.

Files should be marked according to Atea's data classification standards (5 levels). Files marked as strictly confidential must be stored in encrypted format. Files containing personal information must also be marked and maintained according to the GDPR.

Atea employees must be very cautious when storing personal data in files, due to the strict data privacy requirements of the GDPR. Employees must not use personal data in files outside of the original purpose which was defined and communicated to the individual whose data was collected. Employees must limit sharing of files containing personal data to prevent a breach or misuse of this data, and should delete personal data as soon as it is no longer needed. This applies to all files created by Atea employees – including MS Word/Excel/Powerpoint files.

Network security:
Only Atea clients (computers configured according to Atea Standard) shall be connected to the ATEA domain. Atea mobile devices shall only connect to the Atea WiFi network for mobile devices. Other computers or mobile devices are referred to the ATEA-guest WiFi network.

Atea offers employees who are outside of the office the ability to connect to its internal network via Cisco VPN or via Citrix. This allows access to our common file system as well as our common business applications. Connecting to the Cisco VPN requires that the computer belongs to Atea, is a member of Atea's domain (ONE) and has antimalware software installed.

Atea employees should never connect to a customer's network without advance consent from the customer, unless otherwise specified in a customer agreement. The customer should be contacted each time an Atea employee connects to their network, and the Atea employee must always report to the customer what actions they have taken on the customers' network.

Atea employees should be cautious when using public WiFi networks during travel. Data traffic over public networks may be monitored. Before using a WiFi network, Atea employees should confirm that the network is secured and from a legitimate provider. If there is any reason to doubt the security of a public WiFi network, an Atea employee should instead use the mobile network. The Atea Servicedesk can provide support for connecting a PC to the mobile network.

It is expected that Atea employees will use the Internet in their daily work. Private browsing is allowed, but should be limited to sites with content appropriate for the workplace. Online gaming or gambling is not allowed, and file sharing or media streaming through the Internet should be limited to work related content. All employees should be aware that Atea analyzes traffic through the Internet to detect attacks against Atea, and this will also track improper use of the Internet.

When accessing webpages on the Internet, be cautious that the webpage is accurate – especially if you are redirected from another page. Never click links or popups on webpages if they appear suspicious, as these may contain malware which can be loaded on your device.

Communications (email / social media):
Email is a critical digital communication tool for Atea employees. It is also a major source of vulnerability for information security, as it provides attackers the ability to target Atea with malware, fraud and other threats, at low cost and with low risk of prosecution.

One frequent type of identity fraud ("phishing") against Atea occurs when an attacker contacts an Atea employee directly through an email communication. The email appears to be from a trusted source, often by using a false identity

such as that of another Atea employee, a business associate, or a vendor such as a technology firm or bank. The email attempts to deceive Atea employee into a response, such as transferring money, entering login/password data or other sensitive information, or clicking a link or attachment which downloads malicious software ("malware") onto the user's PC or mobile.

The mail, attachment or link will appear to be innocent – for example, will be disguised as a mail from a colleague, an offer/invoice from a vendor or as a notification from a cloud account such as OneDrive. For this reason, Atea employees must be extremely alert to the potential of fraud in any email or other communication, even if the communication appears to be from a trusted source.

Atea employees should never open links or attachments from their devices if they have doubts about the legitimacy of an email or communication. If an Atea employee is uncertain about the legitimacy of an email, or if they have accidentally responded to a possible fraud attempt through opening a suspicious link or attachment, they should immediately contact the Atea Servicedesk to report their concern.

Employee email accounts are frequently targeted by attackers who seek to access an employee's sensitive business files. For this reason, email should not be used for the archival storage of important business information. Business information should be stored or distributed though secured business systems or file sharing solutions, rather than through email.

Private use of email is permitted provided that the use does not conflict with Atea's business interests or interfere with working hours. Private email correspondence should always be appropriate for the workplace, and should be marked "Non-business". In addition, the use of a company email account for personal communication should not leave the impression that the correspondence is in the service of Atea or approved by the company.

Social media is also a frequent communication tool for Atea employees. When used properly, social media provides Atea employees the opportunity to acquire and transfer knowledge, to build commercial relationships, and to strengthen Atea's brand. On the other hand, social media can be highly damaging for Atea and its employees if used inappropriately, or if sensitive information is shared.

Atea employees should therefore be highly cautious about what information they share on social media. Any personal information (including names, photos, etc.) can only be shared on social media posts associated with Atea's business if the person whose data will be shared consents to its use.

Office security:

Atea employees should wear security badges for identification. All visitors to Atea must register at the reception desk, and be equipped with a visiting badge which should be visibly worn. Visitors should be met at the reception at the start of the visit, and followed to the reception to return their badge at the end of their visit. Visitors should not be left alone within Atea premises.

All sensitive information should be removed from desks and securely stored when it is not in use. All whiteboards should be erased of information at the end of meetings. Confidential documents should always be destroyed in document shredders or thrown into special privacy disposal bins when they are no longer needed.

Highlights

Device Security

All Atea PCs, tablets and smartphones should have encryption solutions installed to prevent unauthorized access to the hard drive. Atea PCs, tablets and smartphones should always be watched or stored in a secure location. When not in use, these devices should be locked with PIN/password protection or shut off.

Atea employees should not download software to their PCs that is not sourced from Atea's IT department. If an Atea employee needs to download external software to their PC which is not from Atea, they should first get approval from their manager and from their local IT organization.

Atea PCs are preinstalled with antimalware and firewall applications. If you have any doubt about your antimalware protection, contact the Atea Servicedesk.

If you suspect that your PC has been infected by malware or compromised, first discontinue all work on the computer and disconnect it from the network. Then contact the Atea Servicedesk.

System access

Atea employees should only be granted access to systems when required for their work. Access rights to systems must continually be screened to ensure that this policy is maintained, and that access is terminated as soon as it is no longer required.

File storage

All Atea employees are responsible for ensuring that their work files (e.g., MS Word/Excel/Powerpoint files) are securely managed. Files should be marked according to Atea's data classification standards (5 levels), with a separate marking for files containing personal information. Files marked as strictly confidential must be stored in encrypted format.

All types of files should be stored on Atea internal shared file servers, OneDrive accounts, or the Sharepoint environment. No other external storage sites, including Dropbox or Google Drive, may be used to store Atea files without explicit permission from the country's IT department. Atea employees should not store company information on the hard drives of their local devices.

Network security

Only Atea clients (computers configured according to Atea Standard) shall be connected to the ATEA domain. Atea mobile devices shall only connect to the Atea WiFi network for mobile devices. Other computers or mobile devices are referred to the ATEA-guest WiFi network.

Atea employees should be cautious when using public WiFi networks. Before using a WiFi network, Atea employees should confirm that the network is secured and from a legitimate provider.

Access to the internet from a work device should be limited to sites with content appropriate for the workplace. All employees should be aware that Atea analyzes traffic through the Internet to detect attacks against Atea, and this will also track improper use of the Internet.

When accessing webpages, be cautious that the webpage is accurate – especially if you are redirected from another page. Never click links or popups on webpages if they appear suspicious, as these may contain malware which can be loaded on your device.

Communications (email / social media)

Email is also a major source of vulnerability for information security, as it provides attackers the ability to target Atea with malware, fraud and other threats, at low cost and with low risk of prosecution.

One frequent type of identity fraud ("phishing") against Atea occurs when an attacker contacts an Atea employee directly through an email communication. The email appears to be from a trusted source, often by using a false identity such as that of another Atea employee, a business associate, or a vendor such as a technology firm or bank. The email attempts to deceive Atea employee into a response, such as transferring money, entering login/password data or other sensitive information, or clicking a link or attachment which downloads malicious software ("malware") onto the user's PC or mobile.

Atea employees should never open links or attachments from their devices if they have doubts about the legitimacy of an email or communication. If an Atea employee is uncertain about the legitimacy of an email, or if they have accidentally responded to a possible fraud attempt through opening a suspicious link or attachment, they should immediately contact the Atea Servicedesk to report their concern.

Private use of email is permitted provided that the use does not conflict with Atea's business interests or interfere with working hours. Private email correspondence should always be appropriate for the workplace, and should be marked "Non-business".

Atea employees should be highly cautious about what information they share on social media regarding Atea. Any personal information (including names, photos, etc.) can only be shared on social media posts associated with Atea if the person whose data will be shared consents to its use.

Office security:

Atea employees should wear security badges for identification. All visitors to Atea must register at the reception desk, and be equipped with a visiting badge which should be visibly worn.

All sensitive information should be removed from desks and securely stored when it is not in use.

Holding
Atea ASA
Atea ASA
Brynsalleen 2
Box 6472 Etterstad
NO-0605 Oslo
+47 22 09 50 00
Org.no 920 237 126
investor@atea.com
atea.com

Norway
Atea AS
Brynsalleen 2
Box 6472 Etterstad
NO-0605 Oslo
+47 22 09 50 00
Org.no 976 239 997
info@atea.no
atea.no

Sweden
Atea AB
Kronborgsgränd 1
Box 18
SE-164 93 Kista
+46 (0)8 477 47 00
Org.no 556448-0282
info@atea.se
atea.se

Denmark
Atea A/S
Lautrupvang 6
DK-2750 Ballerup
+45 70 25 25 50
Org.no 25511484
info@atea.dk
atea.dk

Finland
Atea Oy
Jaakonkatu 2
PL 39
FI-01621 Vantaa
+ 358 (0)10 613 611
Org.no 091 9156-0
customercare@atea.fi
atea.fi

Lithuania
Atea Baltic UAB
J. Rutkausko st. 6
LT-05132 Vilnius
+370 5 239 7899
Org.no 300125003
info@atea.lt
atea.lt

Group Logistics
Atea Logistics AB
Smedjegatan 12
Box 159
SE-351 04 Växjö
+46 (0)470 77 16 00
Org.no 556354-4690
customer.care@atea.se

Group Shared Services
Atea Global Services SIA
Mukusalas Street 15
LV-1004 Riga
+371 67359600
Org.no 50203101431
rigainfo@atea.com
ateaglobal.com

ATEA