POLICY ON THE ACCESS OF PARTNERS AND SUPPLIERS TO ATOS IT AND INFORMATION

Content

1. Introduction

1.1. Purpose

This document is a policy, part of the Atos Group Information Security Policies and Guidelines, that is intended for Partners and Suppliers.

This policy defines how access to Atos internal information, Atos customer information and all associated systems by Atos Partners and Suppliers is controlled.

1.2. Scope

This policy applies to all Partners and Suppliers worldwide working with and/or for Atos.

This is a baseline policy and it does not supersede any other document(s) where access to customer information stipulates a higher security constraint (e.g. governments' classified information).

1.3. EU GDPR Compliance Statement

All information which has Personal Identifiable Information (PII) MUST be protected in accordance with EU GDPR controls.

1.4. Intended audience

All Partners and Suppliers of Atos are bound by this policy, the "General policy for all Partners and Suppliers of Atos " in chapter 2 and by all or part of the specific target groups, depending on the nature of the service:

- Partners and Suppliers with a workplace at Atos - chapter 3,
- Partners and Suppliers working on their own systems (e.g. PC, notebook) – chapter 4,
- Partners and Suppliers with a link to resources within the Atos intranet (e.g. online access operations from their own systems) – chapter 5.

It is the responsibility of Partners and Suppliers to enforce the policy also towards any of their Partners, Suppliers as well as their employees who have access to Atos internal information, Atos customer information and associated systems

1.5. Partner and Suppliers responsibilities

To support the efficiency of Atos's business processes, there are occasions where it is necessary to allow Partners and Suppliers access to Atos internal and Atos customer information. This does not reduce the requirement to ensure effective protection is in place to protect against unauthorized access, prevent data loss (including but not limited to, unauthorized copying, deletion, adverse manipulation), or the introduction (malicious or otherwise) of unauthorized software and malware.

Atos Partners and Suppliers MUST instruct their employees to adhere to this policy and implement all necessary controls to check compliance to this by their employees.

Atos Partners and Suppliers MUST flow down the provisions of this policy to their Partners and Suppliers and implement all necessary controls to check compliance to this by their Partners and Suppliers.

Compliance to Atos information security policies is subject to monitoring. Failure to comply may result in Partners and Suppliers being prohibited from entering Atos sites or accessing Atos systems and involve legal consequences and claims for potential damages.

1.6. Keywords

'**Partners'** are companies that share the go-to-market with Atos. In that respect, it can be a supplier, a sub-contractor or a consortium partner.

A "**supplier"** is a non-Atos company which supplies goods and services to contribute to the design, transition, delivery and improvement of services or processes, without a direct link with a prime contract concluded between Atos and a client. It may be distinguished from a contractor or subcontractor, who commonly adds specialized input to deliverables. The supplier definition includes their own subcontractors if any.

A "**consortium member"** is a company associated to Atos to participate in a common activity or pooling their resources for achieving a common goal (specific tender, etc.)

It will participate in both the pre-sales phase of the specific project as well as in the delivery of the Project.

Most of the group's Partners are Software and Hardware Suppliers. Moreover, there are Service Provider helping the group with specific know-how.

'Personal data' is any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity!

'**Shall'**, '**MUST'**, **'shall not'** or **'MUST not'**: strict rule, obligation.

'Should' or **'should not'**: the implementation of these measures is mandatory, except when there are valid business reasons not to do so (e.g. due to technical restrictions and when the deviation is formally documented and approved).

'May' or **'may not'**: optional, to be considered.

2. General policy for all Partners and Suppliers of Atos

2.1. Handling information

1. Regardless of the information type or the medium employed, all information (belonging to Atos or to Atos' customers) MUST be protected by Partners and Suppliers in compliance with its classification level and GDPR requirements.
2. All information which has Personal Data MUST be protected in accordance with EU GDPR controls.
3. In case of processing of personal data, Partners and Suppliers shall ensure they comply with applicable data protection legislations. Partners and Suppliers shall (i) commit to implement adequate technical and security measures to prevent the security of the Personal data and to prevent unauthorized or unlawful processing of Atos Personal data and against accidental loss or destruction of, or damage to, Atos Personal data, and (ii) commit not to transfer Atos Personal Data and/or the performance of the processing of Atos Personal Data to a third party without Atos formal prior approval, even when such transfer takes place for the performance of the service described in this Agreement.
   Once Partners and Suppliers process Personal Data in accordance to EU GDPR and there is no appropriate Data Protection and Processing Agreement yet in place they immediately will give notice to their Atos contact and MUST close an appropriate agreement with Atos.
4. For Atos information that is not in the public domain, there are three protection classes
   - "For internal use";
   - "Confidential";
   - "Secret",

   which are described in Annex 1 "ATOS INFORMATION CLASSIFICATION".
5. In agreement and jointly with the Atos contact and when not explicitly defined, Partners and Suppliers should define the confidentiality level for the information entrusted to them or created by them.

6. Partners and Suppliers MUST protect Atos information. Atos information not in the public domain MUST not be disclosed, shared or communicated to unauthorized parties.
7. For information owned by Atos third-parties (i.e. Atos customer, other partner or supplier), the information must be protected according to the rules defined and agreed with the third-party.
8. Partners and Suppliers MUST take into account the relevant measures drawn to their attention within the framework of their activities or contractual agreements with Atos.
9. Exporting or otherwise trans-shipping Atos/third party information may be subject to the need of export license as per US, EU or national export provisions related to military or dual use terms. If necessary, clarify this with the relevant Atos office, and obtain the appropriate license in a timely manner. Take into account that the export regulations also apply if the information is transferred abroad electronically or via communication networks (e.g. via email or file transfer), or available from abroad on a server.
10. On request of the designated Atos contact, Partners and Suppliers' employees will have to attend the Atos mandatory yearly security awareness session (approximately one hour).
11. Access to information may require, in some contracts, to have Partners and Suppliers' employees signing a Non-Disclosure Agreement (NDA). On request of the designated Atos contact, Partners and Suppliers' employees affected by this requirement MUST sign the NDA proposed by Atos. Any refusal to sign may disqualify the Partner or Supplier's employee to work on the contract.

2.2. System access and admission authorizations

Should Partners and Suppliers be provided with system access and authorization codes to facilitate access to Atos internal information, Atos customer information and all associated systems, it is on the condition that any such usage is made using Atos provided devices unless a connection from a customer owned device or system has been approved by Atos Group Security and is restricted to the agreed framework of tasks or activities. Where possible, Two Factor Authentication Should be the minimum authentication requirement. User Id's (and associated authentication) MUST not be shared by or between Partners and Suppliers' employees.

2.3. Termination of activity

Partners and Suppliers MUST return the following to the relevant Atos office on completion of the agreed activities (unless otherwise agreed):

- The documents and resources passed on to Partners and Suppliers;
- Any information and data media created or used by Partners and Suppliers, including copies and draft versions;
- Partners and Suppliers MUST ensure system access authorizations granted to their employees to undertake the agreed activities are revoked as soon as they are no longer required.

2.4. Deficiencies and incidents

1. Any deficiencies, abnormal behavior of a system, and incidents with information security implications MUST immediately be reported by Partners and Suppliers to the appropriate contacts at Atos.

2. Any loss of information device containing Atos information (or client's information in relation with the contract) MUST immediately be reported by Partners and Suppliers to the Atos contact.

2.5. Statutory regulations

Partners and Suppliers MUST comply with the appropriate data protection legislation, the associated local export provisions and other statutory regulations.

3. Additional rules for Partners and Suppliers with a workplace at Atos

1. Partners and Suppliers MUST take into consideration the relevant information security measures drawn to their attention within the framework of their activities or contractual agreements.
2. A clear desk policy MUST apply. Documents classified as confidential or secret MUST always be protected and placed in a locked drawer or cabinet when leaving a desk (even if only very briefly). All documents, regardless of classification, MUST be stored securely at the end of each day.
3. The removal from the company premises of documents handed over to Partners and Suppliers, the results of work, data media or IT systems is only permissible subject to relevant approval and/or instruction from Atos.
4. The use of the information systems (e.g. PCs, workstations) by Partners and Suppliers is only for the allocated tasks. In particular, the use for private purposes of IT environments made accessible by Atos is prohibited.
5. Partners and Suppliers MUST ensure that systems and access to systems are protected according to security rules communicated in this document or by any other explicit instruction given by Atos.
6. Partners and Suppliers MUST treat the protection mechanisms with due care. Resources such as passwords and smartcards (PKI cards) MUST not be passed on to others or published. They are strictly personal (except while using shared generic IDs, where it has to follow Atos internal approval process).
7. The definition and changing of passwords MUST be made subject to rules that cannot be circumvented. Partners and Suppliers MUST ensure that passwords comply with the following:
   - Formulate passwords from combinations of uppercase and lowercase alphabetic characters, numerals and special characters (at least 3 of above 4 groups MUST be used in the password);
   - Use at least 8 characters, if not applicable the maximum possible number of characters;
   - Change the password at least every 90 days;
   - Do not reuse old passwords;
   - Change the password immediately if there is any suspicion it may has been compromised in any way.
8. When leaving a workstation alone, even if only briefly, Partners and Suppliers' employees MUST secure any open points of access, for example by employing a screen saver or removing the smartcard from the card reader.
9. Where use of the Internet is possible, local regulations and Atos applicable policies MUST be complied with.
10. Security settings, system features or precautionary measures against computer viruses or other malicious software installed on the systems MUST not be disabled, modified or circumvented.
11. In the event of suspected infection by computer viruses that are not automatically detected or eliminated, or if there are problems running virus protection programs, the local Atos contacts MUST be informed without delay.
12. Partners and Suppliers will use Atos e-mail for business purpose only.

13. The use of e-mail encryption is only possible using Atos tools subject to appropriate written agreement and compliance with the relevant regulations.
14. The automatic forwarding of incoming e-mail to external mailboxes, e.g. private e-mail address, external e-mail providers, is NOT permitted.
15. For data archiving and backup purposes, Partners and Suppliers MUST use Atos file servers and Atos backup infrastructures within the Atos network.
16. USB sticks (or any other form of removable media) MUST not be used without the express authorization of Atos and then, only in complete accordance with the Atos Policy on Removable Media.

4. Additional rules for Partners and Suppliers working on their own systems

1. Partners and Suppliers MUST protect their systems against the loss of confidentiality, integrity and availability of all data or information created, processed or stored for Atos, or which is important to Atos.
2. For the purpose of the service delivered to Atos (or to Atos's customers), Bring Your Own Devices are strictly forbidden.
3. Partners and Suppliers will perform their own suitable measures, based on security risk assessments, taking into account at minimum:
   - Data backup (on secured media only);
   - Virus protection;
   - Personal firewall usage;
   - Full disk encryption;
   - System and data access protection.
4. All handover of data to Atos will be conducted only using the agreed procedures and after a complete virus checks with updated signatures.
5. Upon completion of the agreed activities, Partners and Suppliers will securely dispose of all data, documents and data media generated in the course of the cooperation, along with associated copies or data backups.
6. If Partners and Suppliers have no suitable options of their own to ensure the secure disposal of information, documents and data media, they MUST request their Atos contact to assist them by providing access to relevant Atos internal facilities. Data Destruction certificates MUST be provided.
7. Partners and Suppliers MUST not connect directly to the Atos internal network (Atos Intranet) from any non-Atos owned device, without Atos Group Security approval.
8. Access to the Internet will be provided for non-Atos owned devices via the Atos guest network where available.
9. Connections to any external networks from all devices are prohibited at some Atos locations. Permission MUST be sought from the designated Atos host at all sites before attempting to connect.
10. USB sticks (or any other form of removable media) MUST not be used without the express authorization of Atos and then, only in complete accordance with the Atos Policy on Removable Media.

5. Additional rules for Partners and Suppliers with a connection to resources on the Atos intranet

1. Partners and Suppliers MUST only connect to any Atos network, device or service via the technical configuration and the network architecture agreed with Atos, and on the systems provided for the agreed purpose.
2. Partners and Suppliers MUST not build a remote VPN (i.e. IPSEC or SSL) to connect their workstations to any non-Atos network without explicit and written agreement by the Atos IT department.
3. All information about networks and access possibilities (e.g. dialup line numbers, network addresses) and security precautions relating to Atos internal systems and networks MUST be treated as "Atos Confidential" by Partners and Suppliers.

Annex 1: ATOS INFORMATION CLASSIFICATION

ANNEX 1 "ATOS INFORMATION CLASSIFICATION"

This annex specifies the classification attached to Atos Information and how it must be treated through its life from creation to disposal.

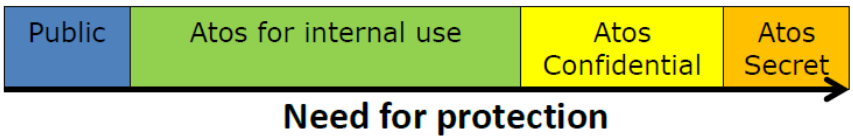
Classified documents belonging to customers must be handled in accordance with the customer's classification standard.

1. ATOS Information Classification Scheme

All information must be classified by the owner or author as either:

1. Public;
2. Atos for internal use;
3. Atos Confidential;
4. Atos Secret.

By default, any information whose classification is not explicitly defined is presumed to belong to the "Atos for internal use" classification.



1.1. Public

Information is defined as Public, if the information has been made available for public distribution through authorized company channels at Group or Local Communications department.

Public information is not sensitive in context or content and requires no special protection.

Examples:

- Atos' Annual Report (after publishing);
- Atos Code of Ethics
- Atos Binding Corporate Rules (BCR);
- Information generated for public consumption such as public service bulletins, marketing brochures and advertisements.

1.2. Atos for internal use

Securing this information is necessary to protect the interests of Atos.

Internal Use information is defined to be of such a nature that outside disclosure would be against the best interests of Atos and consequently must be restricted to use within Atos. Under special circumstances, justified by specific business needs, it may be necessary to share documents under this classification with external third-parties, such as auditors, customers, suppliers or prospects.

Examples:

- operational business information / reports;
- corporate policies, procedures, guidelines and standards;

- internal company announcements;
- detailed and technical documentation of services.

1.3. Atos Confidential

Security of this information is a primary focus.

Confidential information is defined as information of such a nature that the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, could cause damage to Atos by:

- violating the privacy of Atos employees;
- influencing the Atos share price;
- having a negative effect on the delivery of Atos services.

Examples:

- personal data;
- business plans, marketing plans;
- financial information;
- third-party information which is subject to a non-disclosure agreement;
- internal Audit Reports / Intrusion tests results.

1.4. Atos Secret

Security of this information is vital for Atos.

Secret information is defined as information of such a damaging nature that unauthorized disclosure could cause extreme financial damage to Atos or could affect significantly the price of the market share and may result in the imprisonment of Atos management or employees.

Examples:

- financial results before publication date;
- Atos company strategy (e.g. mergers and acquisitions);
- any inside information.

2. Distribution of classified information

For the distribution of classified information, the following rules MUST be applied:

2.1. Atos Public

- Can be share without any restriction.

2.2. Atos for internal use

Can be shared:

- without any restriction within Atos only;
- with third parties under the following guidelines.

  When the information to be shared with a third party that:
  - has a contractual agreement with Atos which includes 'Atos For Internal Use' handling instructions, they must be reminded of their obligations stipulated within the contract;

- does not have a contractual agreement with Atos, it cannot be shared before they are supplied with handling instructions and a Non-Disclosure Agreement has been signed by the third party.
- does not have a contractual agreement with Atos but can demonstrate by written evidence its policy stating that it will handle information as "confidential" and will not allow access to or disclose such information to any other third party.

2.3. Atos Confidential

Can be shared:

- Only to the recipients (Atos group of recipients) specified by the information owner;
- Except in the case of a Project where the team members are listed, the recipient of confidential information may be named or specified by a Group or local distribution list; the distribution list may be of generic nature, as "HR department" or "Customer {X}" (for information shared between Atos teams and a Customer) or a social closed community on internal tools (i.e. blueKiwi);
- The specified recipients are allowed to communicate to some trusted Atos employees a copy of confidential information without reporting to the information owner if:
  - This is justified by operational or business reasons;
  - Each recipient agrees he/she MUST not communicate the information to any other person.
  - This is in accordance with any other process which may apply

2.4. Atos Secret

Only to the recipients specified by the information owner.

The recipients MUST either be named, belong to a local distribution list or to the Project members' spreadsheet.

No further copy or distribution is allowed without the direct involvement of the information owner.