



ATOS SECURITY REQUIREMENTS FOR PARTNERS AND SUPPLIERS

Content

1.	Introduction	2
1.1.	Purpose.....	2
1.2.	Scope	2
1.3.	EU GDPR Compliance Statement.....	2
1.4.	Intended audience	2
1.5.	Partner and Suppliers responsibilities	2
1.6.	Keywords.....	3
2.	General security requirements for all Partners and Suppliers of Atos ...	4
2.1.	Introduction to Charter of Trust.....	4
2.2.	Charter of Trust baseline security requirements for the Supply chain (principle 2).....	5
2.3.	Handling information.....	7
2.4.	System access and admission authorizations	8
2.5.	Termination of activity	8
2.6.	Deficiencies and incidents.....	8
3.	Additional rules for Partners and Suppliers with a workplace at Atos ...	9
4.	Additional rules for Partners and Suppliers working on their own systems	10
5.	Additional rules for Partners and Suppliers with a connection to resources on any Atos network	11
	Annex 1: Atos Information Classification	12



1. Introduction

1.1. Purpose

This document is a policy part of the Atos Group Security Policies and Guidelines (aligned with Charter of Trust¹ security baselines), that is intended for all Atos Partners and Suppliers involved in its digital supply chain.

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.

This document has been written in alignment with [Atos Binding Corporate Rules \(Atos BCR\)](#).

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

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.

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.

¹ For any further information, visit the web site www.charter-of-trust.com



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.

It is the responsibility of Partners and Suppliers to cascade the Atos security requirements also towards any of their Partners, Suppliers as well as their employees.²

A copy of these requirements will be provided to Atos customers upon request to permit them to ensure security alignment with their own policies as well as audits in accordance with contractual conditions.

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. They do not include other partners, included under the name "Sales representatives".

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 partner"** 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 providers 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 For any further information, visit the web site www.charter-of-trust.com



2. General security requirements for all Partners and Suppliers of Atos

2.1. Introduction to Charter of Trust

To make the digital world more secure, Atos and major leading global organizations from private and public sector have joined forces within the Charter of Trust global cybersecurity initiative.

The Charter of Trust represents an unprecedented initiative that establishes three primary goals:

- To protect personal data and business data including sensitive data
- To prevent harm to people, businesses, assets and infrastructure
- To establish a reliable basis where confidence in a networked, digital world can take root and grow

By cofounding the Charter of Trust, Atos promotes the need for cybersecurity awareness and the need to work together to strengthen consumer trust in the digital world. Atos believes that innovative and collaborative end-to-end cybersecurity is a strong asset and competitive differentiator for an organization.

In its Principle 2 (Responsibility throughout the digital supply chain) Charter of Trust has identified 17 security requirements that must be cascaded throughout the supply chain and that are presented hereafter.

It is the expectation of Atos that its entire supply chain will fulfill these requirements.

As part of the delivery of the services by Partners and Suppliers, the delivery against the agreed security KPIs and/or SLAs should be monitored and reported during the Supplier Management reviews, with appropriate improvement actions agreed to address any failure.

2.2. Charter of Trust baseline security requirements for the Supply chain (principle 2)

For all products and services delivered to Atos or to a customer of Atos, the compliance with the following principles are mandatory each time they are relevant (e.g. if personal data is processed, the 1st requirement shall apply, if an incident is discovered the 7th requirement shall apply, etc.).

Suppliers shall agree to incorporate the associated defined KPIs'/SLAs [as detailed in the associated catalogue] into the contract in order to demonstrate their compliance to these 17 baseline security requirements.

<p>DATA PROTECTION <i>Products and services shall be designed to provide confidentiality, authenticity, integrity and availability of data</i></p> <p>1</p> <p>These key principles are not only the foundation of Principle 2 of the Charter of Trust, but are the bedrock of any secure product or service, and should be considered and appropriately implemented early in their design.</p> <p>a. Confidentiality- appropriately protecting data, objects, and resources from unauthorized access, use, or disclosure during processing, storage, and transit</p> <p>b. Authenticity- assurance that data and products come from the source they claim to be from</p> <p>c. Integrity- assurance that unauthorized modification to data or products is prevented</p> <p>d. Availability- assurance that data and products are accessible to authorized parties</p>	<p>SECURITY POLICIES <i>Security policies consistent with industry best practices shall be in effect</i></p> <p>4</p> <p>Mature policies and procedures are critical to provide clear direction to employees on how to operate in a repeatable way, within the confines of an organization's risk tolerance. To that end, organizations should adopt industry best practices that align with standards such as ISO 27001, ISO 20243, SOC2, IEC 62443, or similar trusted standards, to ensure appropriate controls are in place to provide confidentiality, authenticity, integrity, and availability.</p>	<p>INCIDENT RESPONSE <i>For confirmed incidents, timely security incident response for products and services shall be provided to customers</i></p> <p>7</p> <p>Mature incident response policies and procedures are necessary to provide timely response to customers as required by contract, service level agreement, or regulatory requirements.</p>
<p>DATA PROTECTION <i>Data shall be protected from unauthorized access throughout the data lifecycle</i></p> <p>2</p> <p>Data must be protected during all phases of the delivery of a product or service, from creation to destruction, or end of life.</p>	<p>SECURITY POLICIES <i>Guidelines on secure configuration, operation and usage of products or services shall be available to customers</i></p> <p>5</p> <p>Clear and concise directions on how to properly configure, deploy, and operate a product or service are necessary for customers or consumers to fully understand how to secure them.</p>	<p>SITE SECURITY <i>Measures to prevent unauthorized physical access throughout sites shall be in place</i></p> <p>8</p> <p>Mature policies, procedures, and controls are required to prevent unauthorized access to controlled areas such as offices, manufacturing facilities, distribution centers, hosting facilities, labs, etc.</p>
<p>DATA PROTECTION <i>The design of products and services shall incorporate security as well as privacy where applicable</i></p> <p>3</p> <p>The confidentiality and sensitivity of data processed by a product or service must be considered during their design, to ensure appropriate protections are included to prevent unauthorized access, use, or disclosure, and to ensure compliance with any applicable regulatory requirements.</p>	<p>SECURITY POLICIES <i>Policies and procedures shall be implemented so as not to consent to include back doors, malware, and malicious code in products and services</i></p> <p>6</p> <p>Organizations must have Secure Software Development Life Cycle (SSDLC) policies and procedures in place, that can provide reasonable assurances that backdoors, malware, or other malicious code are not included with the product or service, including at the request of a state sponsored actor, criminal organization, or otherwise.</p>	<p>ACCESS, INTERVENTION, TRANSFER & SEPARATION <i>Encryption and key management mechanisms shall be available, when appropriate, to protect data</i></p> <p>9</p> <p>Based on the confidentiality and sensitivity of data stored or processed by a product or service, encryption and key management should be made available for configuration. For example, where data is classified as public, encryption and key management may not be required. However, where data may be classified as confidential, secret, etc., encryption and key management are critical to protect the confidentiality, authenticity, and integrity of the data at rest, in use, and in transit.</p>

ACCESS, INTERVENTION, TRANSFER & SEPARATION **10**

Appropriate level of identity and access control and monitoring, including third parties, shall be in place and enforced

Role based access controls that follow the principles of least privilege, and segregation of duties, are important to prevent unauthorized access to software, systems, infrastructure, and facilities. Additionally, logging and monitoring the activities of privileged users and third parties with access to sensitive data, systems, areas, or facilities is necessary.

INTEGRITY & AVAILABILITY **11**

Regular security scanning, testing and remediation of products, services, and underlying infrastructure shall be performed

Testing such as code scanning and penetration testing must be performed regularly to ensure that any bugs that may compromise a product, service, or underlying infrastructure are mitigated. If a vulnerability is found, remediation should occur in a timely manner, as appropriate to the risk it presents.

INTEGRITY & AVAILABILITY **12**

Asset Management, Vulnerability Management, and Change Management policies shall be implemented that are capable of mitigating risks to service environments

Policies and procedures in three key areas are necessary to enable and ensure the integrity and availability of products, services, and infrastructure:

- Asset Management**- creating inventories and tracking hardware, software, and other assets, both physical and virtual, through the asset's lifecycle, is one of the first steps of any security program.
- Vulnerability Management**- the process of regularly identifying vulnerabilities in software, services, and underlying infrastructure, evaluating their risk, installing patches in timeframes in accordance with that risk, and follow-up scanning to ensure patches are successfully installed
- Change Management**- the process of ensuring all changes are documented, evaluated for risk and security impact, tested and authorized prior to deployment, and tracked through delivery.

INTEGRITY & AVAILABILITY **13**

Business continuity and disaster recovery procedures shall be in place and shall incorporate security during disruption, where applicable

Processes shall be in place to ensure essential products and services can be delivered during, and after, a significant disruption to business operations such as a natural disaster, supply-chain failure, cyber-attack, pandemic, etc., and where applicable, security continuity shall be maintained.

INTEGRITY & AVAILABILITY **14**

A process shall be in place to ensure that products and services are authentic and identifiable

Processes that allow a customer or consumer of a product or service to know that they are receiving exactly what they purchased, not a clone or copy. For example, code signing is a process of digitally signing executables and scripts to guarantee the software has been provided by the author, and not altered or corrupted.

SUPPORT **15**

The timeframe of support, specifying the intended supported lifetime of the products, services or solutions shall be defined and made available

Customers or consumers of a product or service must be able to clearly understand the level of support that will be provided, and the intended life cycle of that product or service.

SUPPORT **16**

Based on risk, and during the timeframe of support, processes shall be in place for: (1) Contacting Support, (2) Security Advisories, (3) Vulnerability Management, and (4) Cybersecurity related Patch Delivery and Support

Based on the confidentiality and sensitivity of data stored or processed by a product or service, processes shall be maintained during the supported lifetime:

- Contacting Support**- there must be a way for a customer or consumer of the product or service to contact support
- Security Advisories**- a method for clearly communicating security advisories to your customers or consumers
- Vulnerability Management**- identifying any vulnerabilities in your products or services, evaluating their risk, and developing patches to remediate them in accordance with the risk they present
- Cybersecurity related Patch Delivery and Support**- a method of delivering patches to your customers or consumers within a reasonable timeframe in accordance to the risk the vulnerability presents, and providing support related to the installation of these patches.

TRAINING **17**

A minimum level of security education and training for employees shall be regularly deployed (e.g., by training, certifications, awareness)

Employees should regularly receive security training appropriate to their job role, to ensure they are aware of formal processes and procedures as they evolve, best practices, changing threat landscapes, and updates to technology.

For more information...
For more information about Charter of Trust Requirements, visit www.charter-of-trust.com

2.3. 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. 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.
6. 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.
7. Partners and Suppliers MUST protect Atos information. Atos information not in the public domain MUST not be disclosed, shared or communicated to unauthorized parties.
8. 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.
9. 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.
10. 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.
11. 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) or demonstrate they have completed an equivalent awareness program internally.



12. 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.

2.4. 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.

2.5. 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 by Atos;
- Any information and data media specifically relevant to Atos created by Partners and Suppliers, unless
 - (i) Partners and Suppliers have to save such information and data in order to evidence ordering and performance of the Services delivered to Atos as legally required or
 - (ii) Partners and Suppliers are allowed by Atos to save the right to retain such information or data by contract or Atos' express approval.
- 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.

If relevant, Partners and Suppliers **MUST** erase any information or data stored on their own infrastructure (including the backup storage) and **MUST** deliver a statement demonstrating such erasure.

2.6. Deficiencies and incidents

1. Any deficiencies, abnormal behavior of a system or similar adverse event **SHOULD** be assessed and managed by the Partner/Supplier's Security team.
2. Any actual or potential incidents with information security implications, this includes but is not limited to
 - data leakage or disclosure,
 - ransomware,
 - loss of information device containing Atos data [or client's information]
 - Failure of security controls

MUST immediately be reported by Partners/Suppliers to supplier-security-incidents@atos.net with as much information available at that time along with contact details of who is handling.

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. Classified documents 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 UserIDs, passwords and smartcards (PKI cards) MUST not be passed on to others or published. The person to whom assigned is fully accountable for all activities relating to the resources.
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 15 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 have 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), unmanaged personal devices and unmanaged collaboration spaces are strictly forbidden to be used for the storage or processing of information.
3. Partners and Suppliers will perform their own suitable measures, based on security risk assessments, taking into account at a minimum the 17 principles detailed in section 2 of this policy, as applicable to the scope of the contract [or subsequent revisions]. The completed risk assessment with compensating controls is to be supplied to the Atos contact.
4. All activities performed in the service of the contract SHOULD be able to be attributable to an individual or automated activity with supporting logs.
5. All handover of data to Atos will be conducted only using the agreed procedures and after a complete virus checks with updated signatures.
6. 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. On the request of Atos, Partners and Suppliers SHALL erase any information or data stored on their own infrastructure (including the backup storage) and MUST deliver a statement demonstrating such erasure.
7. 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.
8. 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.
9. Access to the Internet will be provided for non-Atos owned devices via the Atos guest network where available.
10. 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.
11. 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 any Atos network

1. Partners and Suppliers **MUST** only handle information based on the instructions provided by Atos and the authorizations granted by Atos.
2. 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.
3. 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.
4. 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"

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

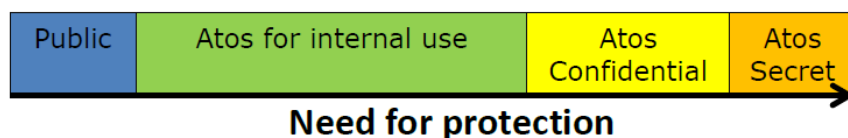
Classified documents belonging to customers must be handled in accordance with the customer's classification standard.

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.