Unify Remote Service Platform

Remote Service Platform v2

Security-Policy for Partner User usage (Issue 1.1)

Trusted Partner for your **Digital Journey**

Atos

1. General

Partner (Company) has to sign a Partner-Contract with Unify Organisation. Within this contract there is also NDA (Non Dislosure Agreement) and GDPR agreement.

Partner (each RSP-user) has an personalized Access to Unify Partner-Portal (SEBA).

2. Only for Partners, working for Unify (Service-Delivery-Partners)

2.1. Legal Rules (Germany)

Every Partner-technican, working for Unify at customer-side or Remote has to sign "Verpflichtung auf das Datengeheimnis nach § 5 Bundesdatenschutzgesetz (BDSG) mit Hinweisen auf weitere Vorschriften zur Wahrung von Geheimnissen"

2.2. Legal Rules (other Countries)

Ensure that the contracts, etc. are signed regarding to your Country-legals

3. General rules

Technical and organizational measures must be implemented at all times and in all locations to protect the workplace against the unauthorized disclosure, manipulation or deletion of sensitive information.

Do not allow unauthorized persons to gain access to sensitive information, whether by copying, spying, or eavesdropping.

Store keys and other authentication devices for accessing IT systems securely at all times; never forward them to unauthorized persons.

Store the access mechanism and password in separate physical locations.

Ensure a level of security that provides suitable protection for information assets, irrespective of the storage medium used. When assessing risks, make no distinction between electronic, physical and other storage media.

Users who become aware of or suspect any irregularity, security incident, risk or error that could damage company assets must discuss the matter with their superior and report it as appropriate. They must take appropriate action to avert any consequential danger and instigate an assessment by competent specialists.

Do not collect, process or use personal data without authorization.

Do not make personal data accessible to unauthorized persons.

Collect personal data only if this is permitted by law or the data subject has issued consent.

Collect personal data only if this is absolutely necessary for the purpose of performing official duties or customer-order

Forward personal data (like Logfiles etc.) to Customers / Partners only after verification and approval by the controller, taking into consideration the local legal requirements and the requirement to obtain the data subject's consent.

4. Handling documents and data storage media

Do not leave sensitive documents or data storage media unattended; always lock them away after use.

After meetings, remove all documents with sensitive contents from the meeting rooms or lock them away.

Protect sensitive information against disclosure during shipment and transmission.

Always supervise the print process personally when outputting sensitive documents to freely accessible printers.

5. Technical Security

Use the implemented update mechanism of your Desktop / Notebooks-Operating System. Every Desktop / Notebook which is connected to RSP must be actual patched!

Do not deactivate the programs made available by the system operators for the automatic identification and elimination of viruses, malware and their update mechanisms, and do not modify their settings. This ensures that the expected level of protection is actually achieved.

If you have administration rights for your workplace computer, you are personally responsible for any changes you make to the configuration and security settings.

If you suspect the presence of malware that cannot be identified or eliminated automatically, or if you encounter problems in executing the antivirus programs, you must inform your User Help Desk or Company-System-Administrator without delay.

6. Accessing IT systems and operating systems

Use the stipulated protection mechanisms for accessing systems and information.

Do not circumvent default security settings, security mechanisms, filters and similar mechanisms.

Whenever you leave the workplace, activate the password-protected screensaver.

Never allow other users to work under your own user ID (on your own PC and RSP-Platform). Implement alternative organizational measures to ensure the availability of data and information in an emergency.

7. E-mail communication

Ensure that the sender's identity is clear for the recipient to see. Do not hide or falsify sender details.

Send confidential and strictly confidential information via encrypted e-mail (like Customer-data etc.)

Do not enter confidential information in the subject line for encrypted, confidential / strictly confidential transmissions.

8. Rules on passwords

Use case-sensitive passwords.

Use a combination of uppercase and lowercase letters, digits and special characters; use at least 3 of the 4 categories.

Do not reuse old passwords immediately.

Do not use trivial passwords containing names or character strings that are easy to guess, especially your user ID. Use different passwords for different security levels and areas.

Comply with any supplementary password rules stipulated by the system operator

Do not forward or disclose passwords intended for personal use to other people. This does not apply to the transmission of temporary passwords to authorized users by the system operator.

Do not share passwords with other people.

9. Rules on entering passwords

Do not allow anybody to watch you enter your password.

About Atos

Atos is a global leader in digital transformation with 110,000 employees in 73 countries and annual revenue of € 12 billion. European number one in Cloud, Cybersecurity and High-Performance Computing, the Group provides end-to-end Orchestrated Hybrid Cloud, Big Data, Business Applications and Digital Workplace solutions. The Group is the Worldwide Information Technology Partner for the Olympic & Paralympic Games and operates under the brands Atos, Atos|Syntel, and Unify. Atos is a SE (Societas Europaea), listed on the CAC40 Paris stock index.

The purpose of Atos is to help design the future of the information space. Its expertise and services support the development of knowledge, education and research in a multicultural approach and contribute to the development of scientific and technological excellence. Across the world, the Group enables its customers and employees, and members of societies at large to live, work and develop sustainably, in a safe and secure information space.

Find out more
about us atos.net
atos.net/career

Let’s start a discussion together

For more information: rsp@atos.net