

DECLARATION OF COMMITMENT

for Access to IT Services of NETWAYS GmbH
and its Affiliated Companies

between

NETWAYS GmbH and its affiliated companies
Deutschherrnstr. 15-19
90429 Nürnberg

– hereinafter „NETWAYS“ –

and

Customer (Organisation)

Company/Authority: _____

Street: _____

Postal Code / City: _____

Country: _____

and the signing natural person:

First name, Last name: _____

E-mail address: _____

Role/Function at the Customer: _____

Project/Contract Number (if applicable): _____

– hereinafter „User“ –

1. PREAMBLE

This Declaration of Commitment governs the obligations of the User in connection with access to and use of IT services of NETWAYS.

It applies to the signing natural person who accesses NETWAYS IT services on behalf of the Customer.

The User undertakes to comply with the following security, data protection, and confidentiality provisions during access to NETWAYS IT services.

2. SCOPE AND PURPOSE OF USE

(1) This commitment applies to all IT services that NETWAYS provides to the Customer and to which the User obtains personal or technical access. These include in particular:

☐ Request-Tracker (rt.netways.de)

☐ GitLab (gitlab.netways.de)

☐ Other IT services: _____

(2) The use of IT services shall be carried out exclusively for the fulfilment of the services agreed between NETWAYS and the Customer and only to the extent necessary for this purpose.

(3) Private use of the IT services as well as any use for purposes other than the agreed business purposes is prohibited.

3. PASSWORDS AND AUTHENTICATION

- (1) Passwords must be at least 14 characters long.
- (2) Passwords must be changed at least once a year and after first use.
- (3) The last five passwords may not be reused.
- (4) Passwords must consist of a combination of upper and lower case letters, numbers, and special characters.
- (5) Default passwords must not be used.
- (6) If multi-factor authentication is provided for an IT service, the User shall use it and treat the required factors with the same level of confidentiality as passwords.
- (7) User credentials assigned to the User are personalised and non-transferable; shared use of accounts is prohibited.

4. URTHUR SECURITY OBLIGATIONS

- (1) Login credentials (e.g. username, password, token, recovery codes) shall be stored securely and not disclosed to third parties.
- (2) The User shall take appropriate measures to prevent unauthorised access to the IT services (e.g. locking the workstation when away, up-to-date virus protection, secure system configuration).
- (3) It is prohibited to circumvent or manipulate security mechanisms (e.g. password policies, session timeouts, access restrictions).
- (4) In the event of a security incident or suspicion of compromised access credentials, NETWAYS must be notified immediately.
Reporting channel:
E-Mail: info@netways.de
Telefon/Hotline: +49 911 928850
- (5) If the User's access is no longer required, the User shall immediately inform the Customer or the responsible parties so that access can be terminated.
- (6) Upon the User's departure from the Customer's organisation or immediately after the end of their employment, access must be reported and terminated.

5. HANDLING OF INFORMATION, CONFIDENTIALITY AND DATA PROTECTION

- (1) The User undertakes to handle all information to which they gain access confidentially and appropriately.
- (2) Personal data shall be treated confidentially and protected in accordance with the General Data Protection Regulation (GDPR) and applicable data protection laws.
- (3) The User shall treat all business and trade secrets of NETWAYS and its customers that become known to them through access as confidential and use them exclusively for the intended purpose.
- (4) Local copies of information (e.g. exports, screenshots, backups) shall only be created if necessary for task fulfilment and are subject to the same confidentiality, protection, and deletion obligations as the original data.
- (5) Access credentials and other confidential information shall be securely and completely deleted after revocation of permissions, unless statutory retention obligations apply.

6. LOGGING AND MONITORING

- (1) The User acknowledges that NETWAYS logs and analyses access to IT services (e.g. login events, configuration changes, data exports) for security, operational, and evidentiary purposes.
- (2) Logging is carried out in compliance with applicable data protection regulations.

7. TECHNICAL OR SYSTEM-BASED ACCESS

- (1) For technical or system-based access (e.g. functional or service accounts) used within the Customer's area of responsibility, the rules stated above apply mutatis mutandis.
- (2) For each such access, a responsible natural person shall be designated. This person ensures that:
 - only authorised persons use the account,
 - access is documented and attributable in a traceable manner, and
 - permissions are reviewed, adjusted, or revoked immediately upon personnel changes or changes in responsibilities.

8. DURATION OF COMMITMENT AND CONSEQUENCES OF BREACHES

- (1) This commitment is effective from the date of signature and for the duration of the User's access to NETWAYS IT services.
- (2) The User is aware that breaches of this Declaration of Commitment may result in civil, employment, and possibly criminal consequences.
- (3) Further contractual provisions between NETWAYS and the Customer remain unaffected.

9. FINAL PROVISIONS

- (1) This Declaration of Commitment supplements existing contracts and agreements between NETWAYS and the Customer without replacing them.
- (2) If individual provisions of this Declaration of Commitment are or become invalid, the validity of the remaining provisions shall remain unaffected.

Place, Date

Place: _____

Date: _____

Signature of User

(User's signature)

Name in block letters: _____

Role/Function: _____