SERVICE DESCRIPTION

17.07.2022

NEPTON

Table of contents

1 General description

Nepton is a comprehensive HR, worktime management and shift planning solution.

Any device with a modern browser is adequate for the use of the service. The service is independent of operating systems and no other software is needed to be able to use it.

Different entry terminals can be connected to Nepton. Entry terminals can be used for entering working time or lunch data.

Nepton can be connected to several payroll, personnel management and enterprise resource planning systems using interfaces. Customers can also establish connections to the service through application program interfaces (API).

Different working time models can be added to the service easily. All the data that has been entered is viewable and reportable including changes. Supervisor's tools for approval and reporting are effective.

Service provider is the company with whom the service agreement was made.

2 Service levels

Nepton includes HR, Worktime management and shift planning modules. Each module is available as Easy, Pro and Complete levels. Service always includes HR module at the selected level. Other modules can be selected as options. All modules include standard functionality.

Service includes:

- Service is available on any kind of device with modern browser
- Single-Sign-On (SSO) functionality
- Calendar integration for registered events
- Programmable application interface (API)
- Standard integrations (for payroll, invoicing, ERP system, call routing solutions, etc)
- Possibility to use entry terminals as cafeteria terminals

Service can be extended with following additional services:

- Managed service
- Elevated SLA
- Test environment. Test environment is an additional environment that can be used by the customer. The setup of the test environment is separate from customers production environment.
- SFTP - server

Provider assists with taking the additional services into use. This can incur additional cost based on the providers price list or on separate project agreement.

2.1 HR – module contains

	Easy HR	Pro HR	Complete HR
Updating of own personal information	X	X	X
Viewing of own work relationship information	X	X	X
Custom permissions	X	X	X
Standard reports	X	X	X
Standard integrations for other solutions	X	X	X
Fixed person- and work relationship information	X		
Custom person- and work relationship information		X	X
Competence management and attaching competence to persons		X	X
Limited storage (5 files / person) for saving documents (work contracts, testimonials, certificates, etc)		X	
Unlimited storage (5 files / person) for saving documents (work contracts, testimonials, certificates, etc) *			X
Online forms (work contracts, development discussions, other forms)			X

*) Service includes normal usage. Normal usage does not cover using the service for other purposes than described in this service description.

2.2 Worktime management – module contains

	Easy Worktime	Pro Worktime	Complete Worktime
Managing own work and absence registrations	X	X	X
Worktime calculations that cover worktime law requirements	X	X	X
Possibility to automate work time calculations for person groups based on worktime law, union agreements or local agreements.	X	X	X
Standard reporting on work time calculations	X	X	X
Flexitime, worktime bank and overtime accruals	X	X	X
Possibility to create standard integrations	X	X	X
Worktime targeting to projects, cost centers, customers, etc		X	X
Holiday and absence accruals		X	X
Holiday and absence planning and reporting		X	X
Travel and expense registration and approval			X
Automatic calculation of allowances on travel registration			X

Unlimited storage for documents and images on events *			X

*) Service includes normal usage. Normal usage does not cover using the service for other purposes than described in this service description.

2.3 Shift planning – module contains

	Easy Shift planning	Pro Shift planning	Complete Shift planning
Shift planning and making lists public	X	X	X
Pre-planned absences and holidays	X	X	X
Shift planning for tasks	X	X	X
Communication of planned shifts	X	X	X
Shift list and levelling period calculation	X	X	X
Standard reporting of shifts	X	X	X
Competence requirements in planning and shift picking by employees		X	X
Shift picking by the employees		X	X
Capacity planning for tasks			X
Shift creation based on planned capacity			X

3 Additional services

3.1 Managed service

Customer can order this additional service to ensure smooth Nepton use in a changing work environment. Managed service includes small-scale modifications to employee user data, user rights, user groups, user setting groups and integration rules. Service request are handled as support level high, if not agreed differently on the individual request.

Named staff of the customer communicates with the managed service.

Managed service includes:

User data:

- Adding persons
- Removing persons
- Employee data changes
- Employee user setting group changes
- Employee user right changes
- Employee user group changes
- Supervisor changes
- Employee unit changes

Work time

- Accrual changes (balance and bank)
- Annual holiday changes
- Work time shortening leave changes
- Length of the workday changes
- User group changes and additions
- User access group changes and additions
- Small-scale user setting group changes and additions
- User work time default project changes

Work shift planning

- Planning templates changes and additions (levelling period model and shift list model)
- Location and unit changes
- Locations changes and additions
- Planning templates changes and additions
- Tasks management

Integrations

- Parameter changes to integrations (for example salary code changes)

Managed service can be taken into use in new service agreements or added to the existing agreement. Managed service will be charged together with the service charge. Managed service cannot be terminated separately.

3.2 Entry terminals

Different entry terminals can be connected to Nepton. Entry terminals can be used for entering working time or lunch data.

For entry terminals, an agreement is in force for a fixed period of 36 (thirty-six) months after which the agreement continues as part of Nepton service agreement. The provider or subcontractor owns the terminals, and the customer has access rights to the terminals and

related software. At the end of the service agreement the customer is obliged to return the entry terminals to the provider.

If there is a fault in the entry terminal, the customer is obliged to deliver the faulty device to the provider's repair shop. The customer is responsible for the delivery cost to the repair shop. The provider will repair or deliver a replacement device in similar condition within the next 5 (five) business days (Mon-Fri).

If the repair shop determines that the fault in the entry terminal was caused by, for example, vandalism, fire, faults or breakdowns caused by air conditioning, electricity or lightning, moisture damage or other similar reason or altered usage conditions or using the device in a way that is not appropriate, the maintenance costs of the entry terminal or the costs of an equivalent product will be charged to the customer.

The provider has the right to deliver the customer a new working time terminal when, for example, when the provider's terminal model has been changed. The delivery costs of the old entry terminal to the provider are the customer's responsibility.

3.3 Single sign-on

Nepton supports several different single sign-on (SSO) methods. In this case, users do not have to enter separate passwords into Nepton. Single sign-on is an additional service that can always be defined separately together with the customer.

Nepton supports Google, Microsoft Azure AD and Microsoft M365 logins.

Nepton also supports standard SAML 2.0 identity providers. Related SSO certificate is owned by the customer. For security reasons, the certificate typically needs to be renewed every few years. Provider tracks pending renewals and will request customer contact person to perform any necessary renewals before current certificate expires.

3.4 Interfaces and integrations

Integrations can be set up by using file downloads, SFTP transfers or by utilizing application program interface (API). The most appropriate method is always agreed upon together with the customer. With an application program interface (API), real-time integrations can be implemented into other information systems.

User guide describes interfaces and integrations in more details.

3.5 Data retainment service

Customer can at the time of service termination order separately invoiced data retainment service. With this service customers information are kept in the service and login credentials are kept active for the duration of data retainment service. Data retainment service gives access to view saved information and does not give usage subscriptions to create additional data or enrich existing data. Data retainment service can be agreed for fixed period.

4 Rules of use

Customer and Provider have agreed the amount of usage subscriptions in the service agreement. Each person how is using the service or whose information is handled in the service needs a usage subscription. Usage subscriptions are agreed to be the amount which is average for the calendar year.

Provided will check the use of usage subscriptions per year. The times when person does not need usage subscriptions is considered when calculating the amount of required usage subscription. For example, organization which needs 100 usage subscription for first half of the year and 50 usage subscriptions for second part of the year will require 75 usage subscriptions per year. Customer and Provider has then agreed 75 usage subscriptions on the service agreement.

If customer utilizes the service less than what is considered normal usage, can this be considered when agreeing the service fee for the usage subscription. This service fee is valid for the time when utilization of the service is less than what is considered normal usage.

If customer uses service as yearly average on higher level what is in the service agreement, then provider can increase the amount of usage subscriptions to match the increased use.

If customer will use service less than their usage subscriptions, the customer must inform the provider about the change 3 months prior to contract period starting.

Provider is responsible for the data protection of the service and the entry terminals, and the operations.

Customer is responsible for the data protection of the computers, devices, systems and telecommunications it uses and its operations in all cases.

5 Implementation

Nepton is offered “As is”. Service includes the functionality for the service level as is agreed on the contact. Implementation does not include changes to the service functionality unless they are agreed in writing as part of the contract.

When doing the implementation, the service is set up to match the customers use case within the scope of the agreed service level. During the planning phase of the implementation the customer will describe their use cases for example organization structure and worktime calculation groups (overtimes and supplements). In the implementation phase the service is set up to match the use cases agreed during the planning phase. Customer is responsible for acceptance testing of the implementation. Acceptance testing will end on the date agreed in the implementation plan, which is followed by required modifications based on acceptance testing findings. After acceptance testing findings are solved, the service will be taken into production use. During production use customer support and help is given by customer service.

6 Support

Nepton support service is available on https://support.nepton.com/hc/en-gb

All service administrators are trained. Trainings form a training path and administrator has a minimum training level of silver. It is possible to earn a certificate which demonstrates the skills learned.

For silver level trained administrators the service fee includes answering questions about use, about the system and its security, about calculations and possible fault reports and reactions to them.

The service fee does not include maintenance of customer's personnel, entries, locations, access groups or projects, making changes to calculation rules, changing system settings, or setting up new calculations groups. These activities are billed separately according to current price list for hourly work, or according to separately agreed managed service agreement.

Provider offers electronic support service, where customer can learn more about the service usage and features. Support service is updated according to changes done to the service.

7 Support availability

Support service is always available.

For trained customer administrators, specialist support is available by email and phone on weekdays between 8 AM - 4 PM. Support requests can be sent at any time via support service or email.

Specialist support availability in more detail can be found in document "SLA normal.pdf".

8 Customer communications

Customers are notified of changes and extensions to the service on the Nepton support or by email newsletters to customers. If they want, customers can opt out of receiving email newsletters.

On urgent situations customer is being informed on the contact points defined by the customer. The contact is made either by using telephone or email. On urgent situation customers are being informed also outside the support normal operating hours.

New features added to the service are communicated in Nepton support or by sending out newsletter for customers.

9 Billing

A service opening fee is charged after the service agreement has been approved. Implementation work is charged as implementation proceeds.

A service fee will begin to be charged on the service implementation date as stated in the project plan or latest when the service is taken into production use. Service fees are charged in advance in periods of twelve months. Service fee is based on the service level and agreed usage subscriptions.

Usage subscriptions are charged on the agreed price on the service agreement. If customers use the service more than agreed usage subscriptions, provider can charge the over-usage. Over-usage is charged based on how much the usage subscriptions have been over-used on average on the calendar year.

10 Continuous development

New version of the service is released on regular interval. New version is taken into use as part of the scheduled new version release. Service development is planned in collaboration with the customers. Customers can affect the development by requesting the functionality that they would like to see in the service.

Nepton has a development plan which describes the topics of changes or new functionality that are going to be implemented in the next 12 months. Nepton uses agile software development methods.

11 Updates, maintenance and availability

Below are the typical times (GMT +2) when routine maintenance tasks will be carried out. It is recommended that automated operations, such as integrations, are not scheduled for these periods.

- **03:00 - 05:30 - Large updates**
  Significant feature changes and longer maintenance jobs. Occurs roughly every quarter. Informed at least two weeks in advance.
- **13:00 - 13:30 - Minor updates**
  Minor changes, fixes, and maintenance jobs. Occurs few times per week. May require users to log-in again.
- **18:30 - 19:00 - Daily maintenance**
  Daily maintenance. May cause short periods of reduced performance, no other impact.
- **22:00 - 24:00 - Security updates**
  Occurs roughly every month. May require users to log-in again.

The service and its components are updated in accordance with the provider's standard practices. Critical data security updates can also be installed outside standard maintenance times.

Service updates have been automated so that the newest version to be implemented must pass many automated tests before installation. This enables continuous quality and functionality improvements.

The availability objective of the service outside maintenance interruptions is at least 99.8%. Availability is measured from several outside measuring points at least 100,000 times a month.

More information about availability and response times is presented in attachment SLA normal.pdf.

12 Supported browsers

The Service works on all modern browsers. Nepton does active development regarding new browser versions so that the service will always work as well and as fast as possible.

Support for Internet Explorer 11 browser in Nepton ended 31st August 2021. You can likely continue to use IE 11 browser even after this date in Nepton, but compatibility is no longer guaranteed, and compatibility has gradually been reducing from autumn 2021 onwards. To get the best experience from the Nepton platform and to maintain your security, you should always use a modern, actively maintained and developed browser, such as Microsoft Edge, Google Chrome, Mozilla Firefox, Apple Safari or Opera.

Service does not use Flash or Java applets.

13 Immaterial rights

No immaterial rights to the service will be transferred to the customer. The customer does, however, have full ownership rights to all the data that it adds to the service and the data that gets developed from it.

14 Data usage rights

Nepton has the right to anonymously utilize data inserted into the service, expect personal information or information that can be considered as personal information, for the purposes of producing the service, statistics, analytics and as learning material towards machine learning and artificial intelligence services.

Personal information or information that can be considered as personal information will only be used on customer's request to solve service tickets.

15 Data management principles

To ensure service quality and to prevent data abuse, customer as data controller or data controller representative authorizes Nepton to collect network identification data of users and to store such data for up to one year.

Data controller or data controller representative can store different kinds of personal information to the service. Such data fields can for example include names, addresses, contact details, bank accounts, social security numbers, tax numbers, emergency close-relative details, job titles, work relationship details, salary details, roles, superior- and subordinate details, cost centers, person identification numbers in various systems, competency profiles, shift plans, sick leaves, holidays, work event recordings and their comments, travel invoices and project relationships. Data controller or data controller representative can also selectively define new data fields to the service and store additional personal information to such fields.

During the contract period, service does not independently remove any data stored by customer or employees. Data deletions performed by customer on user interface or through API typically just move data to the recycle bin, but do not permanently delete data from the service. When storing personal data no longer has legal or operational reasons, customer must request service provider to permanently delete such personal data from the service. Local legislation often defines minimum time periods, in which employee personal data must be stored after the end of work relationship.

When the service agreement is terminated, the customer has the right to obtain its data residing in the service for its own use when so desired. The details of the data transfer and the format will be separately agreed upon at that time together with the customer. The provider charges data transfer working hourly in accordance with its normal price list.

Service provider removes customer and its' employee personal data after the termination of service contract. Retainment of collected data after the termination of service contract is possible via separate service agreement.

16 Protection of personal information

16.1 EU data protection

Regulation (GDPR) aims to improve privacy rights and enforcement of data protection best practices. All organizations managing and handling personal data belonging to EU citizens are affected. Regulatory authorities can impose penalties to organizations not acting as defined in the regulation. Private persons having their privacy rights compromised due to non-compliance can also claim additional compensation from your organization. You can read the full regulation in https://eur-lex.europa.eu/eli/reg/2016/679/oj address.

GDPR enhances data protection and clarifies privacy rights worldwide. Every organization should be aware of the regulation and improve their ways of working as needed. Excellent security and privacy protection reduce risks, creates competitive advantage, and enables new opportunities.

16.2 Nepton data protection

Nepton is known for high data protection and privacy. Several significant customers in finance, law, healthcare, and government have audited and selected Nepton.
Nepton is a centralized location to all personal data. Only authorized persons can access personal data. Customer can fulfill EU data protection requirements by defining the principles of accessing and modifying personal data.

With regards to personal data and applicable data protection legislation, customer is the data controller and service provider is the data processor. Customer is responsible for following

applicable data protection legislation in relation to registered end-users and their personal data.

Service provider handles personal data only to fulfill its contractual and legal obligations. Personal data can for example include employee identification details like name or employee number, information about work time and absences, and all other information which customer needs to manage employee work contracts and to fulfill employer HR obligations.

Service provider agrees to hold personal data confidential and to only handle personal data on customer request. IT 2022 YSE agreement term 7 Confidentiality also covers personal data.

Service provider ensures that service and service provisioning to customer are aligned with applicable data protection legislation, including data protection regulation 2016/679 requirements. Service and service provider data protection can be rated as professional and trustworthy or higher. Service provider ensures the confidentiality, integrity, availability and resilience of the processing systems and services.

Service provider agrees to:

a) handle personal data solely based on documented guidelines from customer, which also applies to transfer of personal data to non-EEA countries.
b) ensure that service provider persons who are authorized to handle personal data have agreed to suitable confidentiality and non-disclosure principles.
c) implement all actions defined in data protection article 32 (Security of processing).
d) follow data protection regulation requirements as applicable to data processor.
e) as possible assist the controller with suitable technical and organizational actions to fulfill controller obligations in answering requests arising from personal data holders.
f) assist the controller to ensure that obligations arising from data protection articles 32-36 are properly followed with regards to handling and scope of personal data.
g) after the termination of contract and as decided by controller, either remove or return all personal data to controller, including all copies, unless EU or member-state legislation mandates otherwise.
h) grant controller access to all information necessary to prove controller compliance with controller obligations, allow controller or controller-appointed auditor to perform audits and participate on such audits.
i) immediately inform controller if any guidance or instruction from controller is deemed to conflict with data protection regulation or other EU and member-state data protection legislation.

Service provider will promptly notify customer about all suspected or confirmed data security breaches, personal data losses or other situations in which data protection of personal data is deemed to be under threat. Service provider grants access to all necessary information about the data security breach and actions which have been taken after the breach. Notification will include at least following information if they are available:

- Nature of data security breach
- Affected persons and types of personal data
- Responsible party behind the data security breach and all other parties who have gained access to breached data
- Repercussions of data security breach

- Actions the service provider has taken and will take to correct the situation, minimize damages and block future security breaches
- Other information necessary for the customer

Service provider agrees to defend customer with regards to all lawsuits, claims, administrative penalties, fines, damages or other repercussions caused by service provider or service provider subcontractor breaking their data protection obligations as defined in this service description or in applicable data protection legislation.

Service provider is not obliged to perform customer requested actions which are illegal.

Service provider transfers personal data to third parties only when authorized by customer. Customer can grant authorization as part of agreement, via documented guideline or by activating or integrating with third-party services. Service provider grants access to personal data through API or other integration mechanism only when authorized by customer.

Customer data will not be transferred outside European Economic Area (EEA).

17 Summary of key technical and organizational GDPR measures

17.1 Confidentiality, Article 32 (1) (b)

Physical Access Control
Data centres are protected by security gatekeepers, access control devices, electric door openers, alarm systems and video surveillance. Office premises are protected by lobby security, electric door openers, alarm systems and external video surveillance.

Electronic Access Control
All passwords and certificates are under central lifecycle management.

Internal Access Control
Successful and failed logins to the service are always logged. Only specific persons have right to view and modify data. Access to data is widely logged and service also widely retains the audit trail of historical changes.

Isolation Control
The service is designed from ground up to offer excellent isolation properties. This is achieved in logical application design & testing level and through centralized isolation & security mechanisms.

Pseudonymization (Articles 32 (1) (a) and 25 (1))
Service as data processor does not offer pseudonymisation options for personal data, as typically all collected data is necessary towards for example HR and/or PAYROLL workflow purposes. Customer as data controller can pseudonymise personal data, or request service provider to pseudonymise data for relevant persons.

17.2 Integrity, Article 32 (1) (b)

Data Transfer Control
All operator network traffic is encrypted.

Data Entry Control
Access to data is widely logged and service also widely retains the audit trail of historical changes.

17.3 Availability and resilience, Article 32 (1) (b)

Availability Control
Online immutable service backups are stored both onsite and offsite. All physical parts of the service have been duplicated, so that the ability of the service to recover from deviations and device faults is high. External networks and power supplies are also duplicated. Backup onsite power supply capacity in the datacentre is 25 MW. All virtual machines are protected by active security scanners and antivirus tools. External and internal firewall are in place.

Rapid Recovery (Article 32 (1) (c))
Nepton has actively maintained and tested disaster recovery plans. Several types of disaster & recovery scenarios have been considered in these plans. Recovery from certain disaster types is automated and causes zero or very short-term interruption to the service delivery. More complex disaster types can require manual intervention by Nepton Ops teams, but these have also been carefully planned to minimize any interruption to the service delivery.

17.4 Procedure for regular assessment, Articles 32(1)(d) and 25 (1)

Data protection management
Data Protection Officer is responsible and coordinates data protection management. Nepton Management Group and relevant teams actively participate in planning, design and implementation of protection measures.

Incident response management
Chief Information Security Officer is responsible and coordinates incident response management. Nepton IT and DEV -ops teams actively participate in any incident responses.

Data Protection by Design and Default (Article 25 Paragraph 2)
From the beginning, Nepton has been developed as a cloud service for many simultaneous customers. Data security and protection on many levels has always been the central design principle of the service.

Processor Control
Nepton has standardised service description, contract and operation model templates towards both customers and possible sub-processors. Such controls are always in place and contractually agreed with all customers and sub-processor chains.

18 Data center

The service is provided from operator's 200 000 server data center. This data center is in Finland and it is extremely energy efficient. All electricity used is renewable and carbon neutral. Heat recycling is used to heat 25 000 households and to reduce carbon emissions by 100 000 tons each year.

Central design principles:

- TIER III EN 50600
- Vahti 2/2013
- ST III KATAKRI
- PUE < 1,2

Standards and certifications:

- Energy Efficiency System + 2014 (EES+)
- ISO 9001 Quality Management (for B2B services)
- ISO 14001:2015 Environmental Management System
- ISO 22301 Business Continuity Management
- ISO 27001 Information Security Management
- LEED Datacenter V4.0
- OHSAS 18001 Occupational Health and Safety Assessment Series
- PCI DSS (Payment Card Industry Data Security Standard)
- SOC 2 (Service Organization Control report type II in 2019)

19 General security practices

The provider uses standardized safety practices that are actively developed and monitored. The provider's management team checks and specifies security requirements, objectives, processes, and methods several times per year. The provider actively promotes the development of safety thinking in its whole organization.

All the provider's personnel have signed a confidentiality agreement. A police security clearance is always performed on those employees in charge of implementation, maintenance and support for customers that require heightened security.

The rights of the service access are determined in advance based on specified access classes. The provider's own personnel's user management and user rights are centralized, so that the risk of erroneous or expired authorizations is minimized. Only provider's personnel responsible for implementation, support and maintenance have access to the system. Provider's support and maintenance personnel adhere to the extreme cautiousness principle and observe only the data and functions necessary for support and maintenance operations.

Customer data in the service is handled and stored only in data centers located in Finland or in another EU country. If the provider starts utilizing data centers outside of Finland in another EU country for the purposes of processing and storing the customer's data, the customer will be notified of this at least 6 months in advance.

An operator in Finland or in another EU country is responsible for conveying messages (text messages and e-mails).

Provider can change data center, telecommunication and other operators. When changes take place, the security level of the service will be kept at the same level.

Nepton acts according to these security principles:

- Data protection: GDPR
- Technical implementation and service: OWASP 2.0
- National security auditing criteria of Finland - KATAKRI II level 4

20 Nepton security

From the beginning, Nepton has been developed as a cloud service for many simultaneous customers. Information security and protection on many levels has always been the central design principle of the service.

Customers' and users' data have been logically separated on all levels of the application's architecture. Each user can only access the information and functions that he or she has received specific rights to.

The service collects information on users' activities at several different levels. Some of the information is saved permanently and some temporarily. In addition to current situation, at least all previous situations, their time stamps and responsible person's identities are saved for all essential entries and changes. The service includes advanced tools for viewing this data.

The service creates a session for each user login. A session is interrupted if the user does not perform any actions in the service for a certain period.

All entries coming from users or external components are checked. This prevents, for example, different injection and XSS attacks.

Servers and components are updated in accordance with the provider's standard practices.

21 Auditing

Nepton service and processes have been audited by several authorities and by, for example, customers in the finance sector. The details of the auditing are always specified confidentially together with the customer.

Customers can audit the service or the source code of the service. In case of source code auditing, the audit is performed at the Nepton premises and with the direction of Nepton personnel.

The customer is responsible for all auditing costs.

22 Logging

Logs are gathered automatically. They are maintained according to principles defined by Nepton data protection officer.

Many data fields in the service are versioned so that full change history is available either through the service user interface or through request to provider support service.

Service gathers logs on multiple levels. General application server logs are retained for at least two weeks. Service gathered logs (for example successful & unsuccessful login and flows in data transfer integrations) are retained for at least two months.

Logs are also available either through the service user interface or through request to provider support service.

Only limited number of technical administrators can access the log management system.

23 Telecommunications

All telecommunications to the service take place with SSL security, except the terminal devices which refresh the current time from online sources on the startup of the device.

Nepton has separate protected networks for visitors, employees, internal services, external services, virtualization, backup networks and network management. Telecommunications between different locations and data centers take place using strongly protected VPN traffic.

Nepton uses several firewalls and other protection systems. Telecommunications between networks is blocked by default and only specified traffic is allowed. Higher-level maintenance networks have been protected with several parallel protection methods. Nepton can follow network traffic and potential deviations.

Data center networks are duplicated. External data center connectivity is provided by four distinct operator fibres arriving from distinct physical directions.

24 Infrastructure

The service is provided on a virtual platform. All physical parts of the service have been duplicated, so that the ability of the service to recover from deviations and device faults is high.

Operating systems and components in use can be moved to other physical devices without service interruptions. For this reason, the planned maintenance of physical devices does not, in principle, cause interruptions in service.

An enterprise-level SAN datacenter cloud stores all service data.

The service consists of several back-end systems and internal components. Users can always see just one unified interface. These back-end systems use their own separate internal networks.

Platform components are updated regularly and as needed. Nepton pays attention to critical data security updates, so that they can be installed as fast as possible. Nepton uses firewalls and security software that protects from malware and intrusions.

The service can include other internal and third-party components:

- Nepton access rights management system
- Data center operator's SAN and information security services
- Telecom operators' SMS and e-mail services
- Third party single sign-on services
- Third party information security certificate services
- Third party NTP time services
- Third party monitoring and sounding services

Telecommunications to services offered by operators and third parties has been protected with strong encryption.

Nepton has several levels of development, testing and production environments. Version updates to all environments are published using continuous integration and implementation automation. This minimizes the possibility for human error and always shortens the duration of planned version update interruptions.

25 Backups

CDP snapshots of the service are taken every hour. These snapshots often represent directly restorable instances and are stored at the data center for 5 days.

IO QUIESCENCE backups of the service are taken at least daily. Backups are kept both at the data center and at another location in Finland in encrypted format. Nepton stores daily backups for 2 weeks and weekly backups for 8 weeks.

Functioning of backups and their integrity are tested regularly.

26 Disaster recovery

If data center or its most vital core systems is destroyed, the service has a:

- Recovery Point Objective (RPO) that is 30 minutes on average and 1 hour at maximum
- Recovery Time Objective (RTO) that is 18 hours on average and 36 hours at maximum

If individual server or device is destroyed, the service can be recovered faster. The recovery is achieved by combining (for example) following activities as necessary for each disaster situation. Some activities can be performed by automation while others are performed by administrators.

- Root cause analysis
- Switching service to another physical platform
- Restoring data storage from earlier CDP snapshot
- Recovering service from backup to original data storage
- Recovering service from backup to new data storage
- Recovering service from SQL DATA+LOG backup to desired RPO moment

27 Changing the service description

The provider has the right to always update IT ETP, IT EHK and IT YSE agreement terms to the latest applicable version.

The provider cannot change these chapters in the service description

- Chapter 9, Billing
- Chapter 13, Immaterial rights
- Chapter 14, Data usage rights
- Chapter 27, Changing the service description
- Chapter 28, Terminating the service agreement
- Chapter 29, Other terms

The provider can change other chapters in this service description. The customer will be notified of important changes at least three months before the new service description becomes effective. If the service description has been significantly changed to the customer's detriment, the customer has the right to terminate the agreement within three months from notification.

28 Terminating the service agreement

Contract is for the calendar year. Contract will be renewed automatically for the next year if contract is not terminated 90 days before the new contract period starts. A fixed-period agreement cannot be terminated to end during the agreement period.

29 Other terms

The provider and Nepton have the right to mention the customer as a reference.

Service pricing is tied to producer price index BtoB-J Q2 of the Central Statistical Office of Finland (https://www.stat.fi/en/statistics/pthi). The provider is entitled to adjust the Service pricing in accordance with the positive index change or 2% per annum. However, the provider is not entitled to adjust the Service pricing during the first agreement year.

Provider and customer have agreed on number of usage subscriptions. If the customer uses the service more extensively than subscribed, the provider has the right to increase the number of usage subscriptions accordingly. Service fee is based on service level and number of usage subscriptions.