Netvisor Information Security Statement

Netvisor is a cloud based financial management software, which is provided as Software as a Service (SaaS). Netvisor-service is provided by Visma Solutions Oy and it's responsible for delivering the service to the customers.

In this document, we have described how Netvisor-service is being delivered to our customers and we also pinpoint the main aspects from information security viewpoint.

Netvisor service delivery

Netvisor-service is hosted by our technology partner Elisa Appelsiini Oy. They are dedicated to provide continuity services for mission critical systems. Elisa Appelsiini data centers are located within Finland and the data centers are certified with ISAE 3402, ISO 9001 and ISO 20000-1 certifications.

Our service availability track record from the previous years has been approximately 99,99%, which means about one hour of unexpected downtime in extended business hours (07.00 - 20.00) during one calendar year. We don't offer any separate SLA for our service to our customers.

Netvisor-service is updated frequently and these updates are performed without service breaks. In certain occasions (eg. updates to our platform infrastructure), we need to have a planned service break. These are performed outside extended business hours and all planned service breaks are informed in advance to our customers through our Community and within the Netvisor service.

Netvisor-service is monitored by our Service Delivery Team and they work closely together with our Customer Service to provide our customers information regarding possible incidents in our service. In case of an incident, we provide frequently updated information to our customers by SMS, in our Community and within our Netvisor service.

Authentication mechanisms and user identity

Netvisor user accounts are always personal and cannot be shared. Netvisor-service uses strong 2FA authentication to identify users. Available authentication mechanisms are TUPAS login from Finnish Banks and strong mobile authentication mechanism from Finnish mobile operators (http://www.mobiilivarmenne.fi/). We also support Estonian ID cards, Swedish BankID and Norwegian BankID for authentication.

Netvisor mobile apps use separate login IDs (email address and password) and these need to be setup through Netvisor UI by the user.

Some limited Netvisor features (including accepting purchase invoices and inputting work hours) are accessible with unique personal direct links. User is authenticated by one-time SMS token sent to user's mobile number. Access to full service always requires strong 2FA authentication.

Security and risk management

Netvisor handles security in several levels including:

- Transport level security in encrypted connections to the service
- Infrastructure security is enforced with common good practises:
    - Network level security: Load balancers, firewalls, network appliances including routers and switches
    - OS and middleware level security: operating system updates, software updates including web servers and database servers, and anti-virus software
    - Application level: mitigation against web application security threats, internal and external web application security auditing, focused on OWASP Top 10

In overall, Netvisor works actively to identify relevant risks and eliminate these risks. Unavoidable risks are controlled so that the total risk level is kept on an acceptable level, while ensuring that the information systems and work procedures remain efficient.

Visma has a separate security team to provide dedicated SaaS security training for all developers and focus is to provide good security threat mitigations to all potential security threats.

Connections to external services

Netvisor-service is connected to multiple third party services to provide our customers automation and useful functionality from our partners. Some of the connections are built-in to Netvisor and these connections are monitored for exceptions and anomalies by Netvisor Service Delivery Team. These connections include connections to major Finnish Banks, government e-services and selected printing services, scanning services and collection agency services. All of these connections use secure protocols for data traffic.

Netvisor-service also has a Web Service API, which our customers can use to implement connections to third party services. All API calls are done over encrypted connections and API authentication is implemented on multiple levels including user and company access checks.

Backups and error recovery

Netvisor-service is compliant with the Finnish laws regarding electronic archiving of accounting materials. Customer data is backed up from Netvisor-service on a daily basis. Backups are stored to a storage system at Elisa Appelsiini. Additionally, the backups are also stored on a separate tape backup system once per day. In the very unlikely event of an major incident, where the current state of database data would be destroyed, maximum data loss would be one business day.

Netvisor offers data recovery services for customers in cases, where there has been accidental changes to the data by the customer's own user or user of a third party partner. In these matters, please contact our Customer Support.

Privacy

All data, which we handle as a data processor, stays always within the EU/EEA area.

We also handle some personal information as a data controller (for customer service, billing, sales etc.) and we use subcontractors (eg. Zendesk) for this. Therefore some personal data may be exported outside EU/EEA area. When using subcontractors, we will always enter into a data processing agreement (DPA) in order to safeguard our customers' privacy rights and to fulfil our obligations towards our Customers.

If the subcontractor is in the US, we make sure that they are certified to the EU/US Privacy Shield framework or we will have a Data Processing Agreement based on the EU Standard Contractual Clauses with this subcontractor. We follow European data protection and privacy regulations and directives and Finnish law and currently we are preparing for the upcoming EU GDPR privacy regulation.

More information

More information about Visma-level standards regarding security and privacy can be found from https://www.visma.com/trust-centre/ and https://www.visma.com/privacy-statement/.

If you have any questions or concerns or you need detailed information regarding our security measures, please contact our Customer Support. Contact details are listed in our Community at https://community.vismasolutions.com/.