Nebu
Pakhuisplein 42V
1531 MZ Wormer
The Netherlands
t. +31 251 31 14 13
nebu@nebu.com

KvK/CoC Zaandam 35022517
BTW/VAT NL800846515B01
IBAN NL96RABO0152190260

Security Statement

Nebu

Our hosting service has ISOs 9001, 14001, and 27001 and NEN7510.

DataCentre:
Intermax Address: Weena Zuid 108, 3012 NC Rotterdam, The Netherlands

Summary
Intermax Hosting is a new state of the art data centre located across The Netherlands, with datacentres in Amsterdam, Rotterdam and Delft. This new state of the art data centre has been designed specifically to meet the growing technical and support needs of our valued hosting customers.

Physical Security
The Data Centre perimeter security contains the following:
- Fencing or other barriers at the perimeter,
- External lighting to deter intruders,
- Security patrols, internal and external at all times
- Security guards at point of entry,
- Closed circuit cameras pointed at the single entry point,
- Alarms on all exterior doors
- Walls extending from true floor to true ceiling to maintain integrity and security of each room,
- Biometric readers at points of entry,
- Secured/locked cabinets

All visitors and vendors are always accompanied when inside the facility, and all visitors are required to sign in and out. If the physical security has been breached an alert is sent to our data centre host. A list of all personnel possessing cards/keys to the data centre is maintained and continually monitored for personnel changes. There is also a process in place to report lost access cards/keys. Building access is logged and reviewed regularly, and access is only permitted to pre-notified and confirmed visitors. The Data Centre is monitored 24/7

Change Management
The Data Centre also runs strict Change Management controls:
- Changes are tracked in a change management system.
- Procedures for changes and emergency changes - for example changes from one incident - described in a manual change management.

Change or addition of components and/or the acceptance of any changes to existing facilities, is made in accordance with the change management process. Procedures for consultation with the client are provided.

Network Security Management
Every connection to an external network terminates at a firewall, these connections are configured to prevent communications from unapproved networks, and to deny access by default.
Security patches are regularly reviewed and applied to boundary devices as appropriate by Nebu's ISP.
Monitoring tools are deployed and configured in critical segments to detect compromise of network security, as well as to ensure minimal downtime/disruption to services.

Internet
Monitoring tools are deployed and configured at the point-of-presence to detect compromise of network security, via external Internet access.

Access to Nebu's Internet programs are password protected and restrictable by the client.
Cati stations are required to be registered with the Nebu system, logging their IP address before access can be granted to read from a survey and write survey related data.
Cati stations can be password protected as can Interviewers
The connection used between the servers is based on a local network configuration to reduce possible external attacks on the transfer of data between the IIS and SQL servers.

Wireless

Wireless access is not possible or permitted within the data centre.

Audit Logging

Logs are generated for security relevant activities on network devices, operating systems and applications. These are used to enable audit tracking and incident control.

Access Control

Initial access to the Nebu software is controlled by Nebu. Access rights can be granted by the client, but the control over the issue of these rights is the client responsibility, and Nebu accept no responsibility whatsoever over the use of these rights.

Penetration Testing

In order to comply with data protection issues Nebu has not undertaken penetration testing itself on its accounts, but many clients have, and have reported no issue that was not remedied as part of the continuous maintenance to date.

In addition, Nebu have also checked for vulnerability from a possible respondent entering SQL commands within the text verbatim.

Data Protection:

According to the Safe Harbor agreement all EU companies are, by default, members of the agreement: The agreement establishes a framework for a compromise solution between U.S. and E.U. privacy procedures.

However, there is a requirement for all companies under the Safe Harbor agreement to adhere to the EU Directive on Data Protection. This states that:
The responsibility for compliance rests on the shoulders of the "controller", meaning the body which alone or jointly with others determines the purposes and means of the processing of personal data; (art. 2 d)

The data protection rules are applicable not only when the controller is established within the EU, but whenever the controller uses equipment situated within the EU in order to process data. (art. 4). Controllers from outside the EU, processing data in the EU, will have to follow data protection regulation.
Therefore, any company outside the EU using Nebu's hosted solution would need to ensure that they complied with the Directives requirements regarding the transfer of data.

'Safe Harbor stipulations require that: companies collecting personal data must inform people that the data is being gathered, and tell them what will be done with it; they must obtain permission to pass on the information to a third party; they must allow people access to the data gathered; data integrity and security must be assured; and a means of enforcing compliance must be guaranteed.'

The EU Directive goes further and stipulates that:
'Personal data should not be processed at all, except when certain conditions are met. These conditions fall into three categories: transparency, legitimate purpose and proportionality.'
The Directive gives an extensive description of the categories and their application.

Thus, Nebu are members of the safe harbor agreement, being members of the EU, and are also obliged under the EU Directive to conform to regulations regarding the handling of personal data. However, it is the duty of the Client (as controller of the data) to ensure that the regulations are upheld.

The Nebu Team