Nebu B.V.
Pakhuisplein 42 V
1531 MZ Wormer
The Netherlands
T: + 31 251 311 413
E: nebu@nebu.com
W: www.nebu.com

Nebu Security Statement

Reference	:	Nebu - I - 2016 - 0089
Version	:	v1.2
Date	:	September 9, 2019
Owner	:	Zoltan Szuhai - Security Officer
Validation:	:	Otto van Linden
Status	:	Final

CONTENTS

Version Control			
Version	**Status**	**Date**	**Change Log**
V1.0	Final	November 7, 2016	-
v1.1	Final	January 5, 2017	Minor updates
v1.2	Final	September 9, 2019	Minor updates

1 Introduction

Nebu is a leading supplier of quantitative data collection software. Ensuring our platform remains secure, is vital to protecting your data and information with the highest priority.

Our security strategy covers all aspects of our business, including:

- Nebu general security policies
- Physical and environmental security
- Operational security processes
- Scalability & reliability of our system architecture
- Systems development and maintenance
- Service development and maintenance
- Regularly working with third party security experts

2 Nebu General Security Policies & Procedures

Every Nebu employee signs a Data Access Policy that binds them to the terms of our data confidentiality policies. Access rights to the systems are based on employee's role.

3 Security in our Software Development Lifecycle

Nebu adheres to the Nebu Development Security Standards during development. This policy covers project management of development items, development stages, development and test environment security, source code protection and security, coding and software design related security, employee human aspects, documentation rules and support related security considerations. The Nebu Development Security Standards document also declares, at process level, the internal security and vulnerability test of every major release and the regular penetration test of Nebu products, conducted annually by an independent third party security company.

During the application development, the created codes undergo a continuous integration system, and several different level integration and automated tests are executed against the whole software package. Software development works closely together with the system administrator team to guarantee highest level security and build common knowledge.

4 Security at the Nebu offices

Nebu offices adhere to the Nebu Information Security Management System, which covers security from physical aspects as well as the technical restrictions. Employee related security regulations are declared within Work Contracts and by the Human Resources Security policy.

5 Software Architecture & Scalability

Nebu systems are available on premise and as a hosted solution. Hosted solution is available via dedicated virtual servers (Dub InterViewer and Dub Knowledge) within a secure environment, where the virtualized environment guarantees high availability, optimal resource management and the possibility of resource adjustments on the fly, as well as regular backups created. Nebu Data Hub is hosted on scalable Azure SQL service, with regular backups, with scalable server setup. In both hosted cases, the location of the data and the servers are known, and bound to a region or data centers.

6 Encrypted Transactions

Web connections to our servers are via TLS 1.0 and above, weak ciphers are disabled by default.

7 Information Security

7.1 Workstations, Notebooks, Tablets and Mobile Devices

All laptops and workstations are secured via installed virus scanner, that reports centrally about the up-to-dateness of security patching and possible infection state of a machine - this solution also includes active host intrusion prevention system. Authorised Nebu personnel have the ability to remote wipe a single, or set, of machines (phone, tablet, notebook). Workstations, notebooks, tablets, mobile devices have their disk encrypted and, of course, by default all machines are password protected. Workstations are further protected within the office network infrastructure and apart from software and operating system maintenance, those are protected with regular physical maintenance as well.

7.2 Application Review

We work with an independent security company to review and tweak further our applications. Any used 3rd party applications are regularly updated to have a secure, stable environment.

8 Data Center Security

All servers have virus scanner installed including active host intrusion prevention system. The system is annually reviewed by a 3rd party security company. Nebu guarantees regular maintenance of the servers and services for optimal security.

8.1 Intermax

Intermax is our trusted partner, where security is a core value. For key security characteristics please visit Intermax website.

8.2 Azure

Microsoft Azure platform is an industrial leader hosting service and application service platform. For key security characteristics please visit Azure website.

9 Product Features

9.1 Administrator and Management Features

- Administrator users can only access the system upon authentication
- No functionalities are accessible without login
- Administrators can manage users and their access rights to functionalities, as well as define the renewal frequency for user passwords to be refreshed.

9.2 User Features

- All users of the system need to log into the system
- No functionality is accessible without login
- Functionality, that can be used by a user, is configurable by the administrator user

10 Availability

Availability of our systems to our customers is key. Systems are monitored at hardware and service level, where metrics are regularly evaluated, and if needed necessary tuning or adjustment of the systems are executed.
Applications and application performance, applications logs are also monitored, collected, and regularly evaluated. Collected data is evaluated by System Administration, Development and Customer Care.
In our solutions and our approach to new functionality, highest possible availability is always evaluated, as a non functional requirement towards the product or service.
For used hosting partners and for Nebu, there are explicit business continuity plan(s).

11 Where to report a security concern?

Please contact our Customer Care department.