180122

JEEVES
INFORMATION SECURITY POLICY

1. General Jeeves' Information Security Policy

The purpose of this document is to give Jeeves' customers licensing the Jeeves products or purchasing the functionality of the Jeeves products through a "Cloud" or other service hosted by Jeeves ("Customer"), from Jeeves or a Jeeves distributor ("Jeeves Partner"), an overview of the security considerations of Jeeves, both from a process and product perspective. Jeeves Managed Service Partners are in this context Customers to Jeeves.

Jeeves maintains an information security standard in accordance with Jeeves' established policy.
Jeeves' Information Security Policy is a process in constant development taking into consideration the Jeeves products and the "*state of the art*" regarding IT security.

The policy applies to all Jeeves employees and sub-contractors and covers products, development, product support and, as the case may be, professional services or "*Cloud services*" performed and supplied by Jeeves.

The policy further covers all manual and electronic processing of Jeeves' information as well as of Customer's and/or Customer's client's information in the case such information is processed or stored in Jeeves' internal IT environment or on Jeeves' premises.

2. Confidentiality

2.1 Definition Confidential Information. As used herein, "Confidential Information" means all non-public information, whether in oral, written or other tangible form that the party disclosing the information (the "Disclosing Party") designates as being confidential or which, under the circumstances surrounding disclosure, the receiving party (the "Recipient") knows or has reason to know should be treated as confidential, including without limitation, the terms and conditions of this Agreement.

2.2 Exclusions. Notwithstanding the foregoing, Confidential Information does not include information that: (a) is or becomes generally available to the public other than (i) as a result of a disclosure by Recipient or its employees or any other person who directly or indirectly receives such information from Recipient or its employees or (ii) in violation of a confidentiality obligation to Disclosing Party known to Recipient; (b) is or becomes available to Recipient on a non-confidential basis from a source which is entitled to disclose it to Recipient; (c) was developed by employees or agents of the Recipient independently of and without reference to any information communicated to Recipient by the Disclosing Party; or (d) is required by law to be disclosed by the Recipient. A disclosure of Confidential Information which is (x) in response to a valid order by a court or other governmental body, (y) otherwise required by law, or (z) necessary to establish the rights of either party under the Agreement, shall not be considered to be a breach of obligation or a waiver of confidentiality for other purposes; provided however, that the party disclosing such information shall provide prompt written notice thereof to the other party to enable it to seek a protective order or otherwise prevent such disclosure.

3. MANAGEMENT AND CONTROL OF ACCESS RIGHTS

3.1 Authorization and Authentication

3.1.1 Users will only be given sufficient rights to all systems to enable them to perform their job function. User rights will be kept to a minimum at all times.

3.1.2 Users requiring access to systems must make a written application on the forms provided by the IT Department.

3.1.3 Where possible no one person will have full rights to any system.

3.1.4 The IT Department will control network/server passwords and system passwords will be assigned by the system administrator in the end- user department.

3.1.5 The system administrator will be responsible for the maintaining the data integrity of the end-user department's data and for determining end-user access rights.

3.1.6 Access to the network/servers and systems will be by individual username and password, or by smartcard and PIN number.

3.1.7 Usernames and passwords must not be shared by users. Usernames and passwords should not be written down.

3.1.8 All users will have an alphanumeric password of at least 10 characters. Jeeves are following general guidelines published in "NIST Special Publication 800-63. Appendix A".

3.1.9 The user account will be locked after 10 incorrect attempts.

3.1.10 The IT Department will be notified of all employees leaving the Organisation's employment and will then remove the employees' rights to all systems.

3.1.11 Network/server supervisor passwords and system supervisor passwords will be stored in a secure location in case of an emergency or disaster.

3.1.12 Use of the Administrator username on Windows is to be kept to a minimum.

3.1.13 Default passwords on systems such as SQLServer will be changed after installation.

3.1.14 File systems will have the maximum security implemented that is possible. Where possible users will only be given Read and Filescan rights to directories, files will be flagged as read only to prevent accidental deletion.

3.2 Incident handling

3.2.1 Any security breach and/or personal data breach being detected will within 24 hours be sent to Head of IT for further handling and decision on whom to inform. The information is to contain information of the breach, personal data records affected, consequences and how the breach can or has been solved.

4. VIRUS PROTECTION

4.1 The IT Department will have available up to date virus scanning software for the scanning and removal of suspected viruses.

4.2 Corporate file-servers will be protected with virus scanning software.

4.3 Workstations will be protected by virus scanning software.

4.4 All workstation and server anti-virus software are automatically updated with the latest anti-virus patches.

4.5 No disk that is brought in from outside the Organisation is to be used until it has been scanned.

4.6 All removable media containing executable software (software with .EXE and .COM extensions) will be write protected wherever possible.

4.7 All demonstrations by vendors will be run on their machines and not the Organisation's.

4.8 Shareware is not to be used, as shareware is one of the most common infection sources. If it is absolutely necessary to use shareware it must be thoroughly scanned before use.

4.9 New commercial software will be scanned before it is installed as it occasionally contains viruses.

4.10 All removable media brought in to the Organisation by field engineers or support personnel will be scanned before they are used on site.

4.11 To enable data to be recovered in the event of a virus outbreak regular backups will be taken by the IT Department on data stored in the Jeeves Internal inhouse IT environment

4.12 Management strongly endorse the Organisation's anti-virus policies and will make the necessary resources available to implement them.

4.13 Users will be kept informed of current procedures and policies.

4.14 Users will be notified of virus incidents.

4.15 Employees will be accountable for any breaches of the Organisation's anti-virus policies.

4.16 Anti-virus policies and procedures will be reviewed regularly.

4.17 In the event of a possible virus infection the user must inform the IT Department immediately. The IT Department will then scan the infected machine and any removable media or other workstations to which the virus may have spread and eradicate it.

5. JEEEVESERP PRODUCT DEVELOPMENT

5.1 Coding Guidelines and Reviews

5.1.1 Jeeves R&D are following code conventions specific for each language such as e.g. c#, Delphi and Java. To aid us in our development Jeeves R&D are also enforcing code conventions with third party programs, e.g. Resharper or IDE built in features.

5.1.2 Throughout the development process Jeeves R&D are performing code review for a major part of Jeeves developed code.

5.1.3 New developers go through a certification process where patterns used during development are covered to ensure the same pattern implementations.

5.2 Quality system for development of JeevesERP

Jeeves follow Kaizen, Kaizen means continuous improvement.
Continuing improvement involves everyone – managers and workers alike. Kaizen is implemented by improving every aspect of a business process in a step by step approach while gradually developing employee skills through training education and increased involvement. For us that means working together with our clients (and our own team) on the software development life cycle.
Our development methodology deeply supports Kaizen. The scheme for this support is the following: we plan, we do, we receive some feedback on what is done, and based on this feedback we improve.

5.3 Testing procedures for the development of JeevesERP

Jeeves follow the Agile Scrum methodology for development of JeevesERP. There are multiple levels of rigorous testing involved in Agile that Jeeves are following.

6. PROCESSING OF CUSTOMER OR CUSTOMER'S CLIENT'S DATA

6.1 Scope

The following rules apply in situations where Jeeves have access to and processes Customer data or Customer's client data while for example performing support of the Jeeves products or when Jeeves supplies the Jeeves products through "Cloud" or other services to Customer or Customer's clients.

6.2 Ownership of Customer or Customer's Client Data

Each party undertakes to treat the personal data of the other party in accordance with applicable local law and in accordance with the other party's reasonable instructions, further, to take such technical and organizational measures required to protect the data processed from unauthorized access, destruction and alteration.
When processing Customer's or Customer's client's personal data during performance of either support or "Cloud" or other services," the Customer shall be considered as "personal data controller" (sv. *Personuppgiftsansvarig*) and Jeeves or subcontractor as "personal data assistant" (*sv. Personuppgiftsbiträde*). This means that Customer shall at all times be liable for and have the right of instruction regarding the processing of the personal data and the manner in which such processing is performed.
Customer's instructions regarding the processing of personal data shall be given in writing to Jeeves. Jeeves undertakes to assist Customer should any individual who's data is registered, request access to information of personal data registered or request correction of such data.
To the extent required by law, Jeeves shall, at Customer's request, enter into an agreement as personal data assistant (sv. *Personbiträdesavtal*) with Customer on terms as reasonably acceptable to Jeeves.

6.3 Access to Customer's System for Support and Consultancy services

6.3.1 Customers are to provide remote control and/or VPN connection of a type that can be approved by Jeeves IT Department, to the Customer's Jeeves client and system environment. The conditions for remote access to Customer's Jeeves client and system environment such as valid login information should be made available to Jeeves.

6.3.2 Customer shall have appropriate information security protection in place, as set forth by legislation, regulations and industry best practice. (e.g. Security administration routines for malware protection, Patch management, User authentication, Access control, Confidentiality protection, Incident detection, Log management , Disaster recovery, Key management, Network security management and Physical protection of IT-resources).

6.4 Protection of Data

All Customer data (being stored at Jeeves) is to be treated according to this policy.

7. RULES REGARDING "MANAGED SERVICE", HOSTING OF INFRASTRUCTURE

7.1 Amazon

The Jeeves Cloud Service is hosted at the AWS. The terms and conditions for such cloud services can be found on:

http://aws.amazon.com/agreement/
http://aws.amazon.com/partners/terms-and-conditions/

Customer shall abide by and follow all the terms and conditions for use of the AWS. Jeeves does not guaranty Amazon Web Service, Inc's obligations pursuant to such terms and conditions, nor can Jeeves grant any additional terms required by the Customer in excess of what are offered by Amazon Web Services, Inc., nor any terms in contradiction of such terms and conditions.

7.2 Additional Terms

All additional terms are regulated in the Jeeves Cloud Managed Services agreement.

9. DISASTER RECOVERY JEEVES INTERNAL PRODUCT PRODUCTION ENVIRONMENT

All applications hosted by Jeeves IT and classified with a business value of 1 are replicated on a daily basis (some systems are setup with a replication of business critical data 1/day) to another datacenter from the datacenter running the applications.