2021

Continia Software

INFORMATION SECURITY MANUAL

CONTINIA ONLINE SERVICES

DOCUMENT: IT SECURITY MANUAL FOR CONTINIA ONLINE SERVICES.

LAST REVISION: 5.0

AUTHOR: TORBEN KRAGELUND.

CO-AUTHORS: HENRIK LÆRKE, TOMMY LYDIKSEN, JENS TOFTEGAARD BOESEN, GITTE SKAARUP NIELSEN

BE DISTRIBUTED TO: DEVELOPMENT, OPERATIONS DEPARTMENT AND SUPPORT DEPARTMENT.

CONTENT

5 IT SECURITY MANUAL FOR CONTINIA'S ONLINE SERVICES

5.1 INTRODUCTION - PURPOSE AND SCOPE

The purpose of this IT Security Manual is to provide information to Continia Software's customers and auditors regarding Continia's implementation of the international audit standard for declaration tasks on controls at a service provider, ISAE 3402.

In addition, the purpose of the document is to provide information on the controls used for operation and information security with us between 1 January 2020 and 31 December 2020.

The following description includes the control objectives (Security Measures) and Controls (Implementation Guidelines) at Continia Software A/S, which is in place for the majority of our customers and are based on our standard delivery. Individual customer relationships are not included in this description.

5.2 CONTINIA SOFTWARE A/S AND OUR ONLINE SERVICES

Continia develops and delivers software products to Continia's reselling partners and end customers globally. As technology evolves, these products contain more and more online services and data exchange between customers and services. The number of exchanges and the amount of data are expected to increase in the future.

Continia's products and related online services are business critical to Continia's customers and many customers are demanding security for data processing and operational security/stability.

Continia aims to provide reliable and data-secure online services as part of Continia's products. This security policy focuses on the online services and the supporting operation.

The policies should at least meet and support the requirements Continia undertakes at any time in the license terms of the Continia products (Appendix A).

Furthermore, policies should meet the requirements of Danish and EU legislation for data protection and security (Appendix B).

5.3 ORGANISATION AND RESPONSIBILITY

Continia Software A/S employs approximately 60 people. The management is generally responsible for Continia's IT Security, which is prepared and maintained in cooperation with the company's IT Security Committee. Operation and maintenance of the Online Services is provided by employees in the development department. The development department also acts as 3rd line support for hotline support and handles customer questions/error reports in connection with the online services.

The IT security strategy, supporting documentation and systems, can be found on the company's central IT Security Portal, where relevant access rights, change notification and audit trail are also managed and maintained.

5.4 Risk Management in Continia Software A/S

We have an ongoing risk assessment of our business and especially our Online Services. In doing so, we can ensure that the risks associated with the services we provide are minimized to an acceptable level.

Risk assessment is carried out periodically (minimum every 6 months) and when we make changes or implement new services. Responsibility for risk assessments lies with our IT-Security responsible.

5.5 General about our control targets and implemented controls

We have defined our quality management system based on our overall goal of providing stable and secure online services to our customers. In order to do this, we need to have policies and procedures in place to ensure that our deliveries are uniform and transparent.

Our IT security policy is prepared with reference to the above and applies to all employees in the company and especially to relevant employees in the development department.

Our methodology for implementing controls is defined by reference to the ISO 27002 (Information Security Management Framework), and is thus generally divided into the following control areas:

- General guidelines
- Organizing information security
- Employee safety
- Information-related asset management
- Access Management
- Cryptography
- Network security
- Development and Maintenance of Online Services
- Subcontractors
- Managing security events
- Emergency management
- Compliance with statutory and contractual requirements.

We continuously improve policies, procedures and operational operations.

5.6 Control environment

The following describes our control environment in more detail for each area. Where the security measures we set are the desired goal and the implementation guidelines are the way to ensure we comply/can check if we are achieving the goals.

5.7 General guidelines

We have defined our overall methodology and approach to delivering our services with what it means in our IT security strategy and associated supporting documents.

The purpose is to ensure that we have management-approved information security guidelines in relation to the business strategy — and in relation to relevant legislation. Management's guidelines are communicated to all employees of Continia Software A/S, and we continuously update the documents as needed, and at least once a year.

This topic is further described earlier in this description, under the heading 'General about our control targets and implemented controls'.

6 ORGANIZING INFORMATION SECURITY

6.1 INTERNAL ORGANIZATION

We have established an IT security strategy that describes how to deal with IT Security in our business and our Continia Online Service delivery. All employees are aware and trained via the intranet or other company initiatives and are informed when management approves updates to the strategy.

Confidentiality is generally established for everyone involved in our business. This is done through employment contracts or cooperation agreements with subcontractors and business partners.

In the case of parties that are an integral part of our deliveries, we must supervise the subcontractor's established controls.

Our internal IT security implementation that ensures that strategies and procedures are updated and contribute to the optimization of the current level of security in Continia Software A/S. An internal evaluation of information security is carried out on an ongoing and at least annual basis. In addition, the evaluation is carried out by an external IT auditor as well as in connection with the preparation of the annual ISAE 3402 declarations.

6.1.1 Roles and responsibilities

Everyone in our company must live up to the role assigned to them and follow our procedures as set out in our IT Security Manual. This is to ensure that, among other things, the related matters are escalated and addressed. Most importantly, we ensure stable operation, protecting our customers' data, our equipment and thus our business. The role and responsibility description, including tasks and responsibilities in relation to security, is defined in the prepared role descriptions, the employees' employment contract and in the IT Security Manual.

It is the management that approves the guidelines for strategies and procedures, and it is the management who periodically approve updates to this. This is carried out annually to ensure an up-to-date strategy.

Security measure

- All employees are informed about the IT Security Strategy.
- All security documentation is stored centrally and all relevant information is available to all employees.
- Review of comments/updates is stored on the company's IT Security portal as documentation.

Implementation guidelines

- Changes are communicated to all employees, minimum on the annual company day.
- Quarterly, new employees are introduced to IT Security.
- A central IT Security portal with different rights groups is implemented.
- Review and versioning are implemented on all procedures.

Comments

- An area is created where HR relevant information can be stored and where only HR and Director has access.

6.1.2 Functional separation

Definition of roles and responsibilities in relation to IT Security:

Role	**Responsibility**
CEO	Overall IT Security Responsibility Ensure delegation of IT Security responsibilities and roles Secure allocation of resources (time and budget) HR responsibility
IT Security Committee	Group of relevant employees appointed by the Director to represent relevant parts of the company. Responsible for preparing and following IT security policy and overall procedures.
HR	Responsible for employee/employment related matters. Ensure documentation for the recruitment and storing of relevant documents.
Internal IT	Responsible for security around internal IT, purchase of hardware and software, internal PCs, Servers, Backup, Networking, connectivity, software, user and access management, disposal. Cooperation with and evaluation of external suppliers to Intern-IT
COS Operations Manager	Responsible for security around operation, data and maintenance of Continia Online Services Responsible for deployment of new functionality to live environment. Cooperation with and evaluation of external suppliers with deliveries to support Continia Online Services Follow-up on IT Security incidents
Employee in Development Department	Design, development and testing of secure and operational stable software.
Other employees	Compliance and support for Continia Software A/S's general IT security policy.
IT Security Manager	Follow-up and system support for IT security policy, manual and implementation. Monitoring IT security implementation. Responsibility for execution to risk assessment.
Solution Manager	Ensure implementation of new functionality does not compromise data security and operation stability according to the company's security strategy including applicable laws such as the Personal Data Act and the EU GDPR. Continuous evaluation and optimization of process for design, development, testing and live deployment.

Security measure

- Roles and responsibilities are defined to ensure continuous follow-up.
- Roles and responsibilities are made visible to everyone in the company.
- Roles, responsibilities and related employees are assessed annually by management.

Implementation guidelines

- Employee is informed about roles and responsibilities by their manager, at least once a year.
- Roles and responsibilities are described on the IT Security Portal.
- The IT Security Committee updates and maintains roles and responsibilities at the direction of management.

Comments

- In assessing risk, relevant roles and responsibilities should be assessed at the same time, as many risks and management will be related to roles and responsibilities.

6.1.3 Contact with authorities and interest groups

Requirements and expectations for IT Security change continuously – both in terms of change in regulatory requirements, technological development and market/industry needs. These requirements and expectations are important to get into Continia Software's IT Security Strategy, Risk Assessment and IT Security Management.

Security measure

- IT Security Manager stay to date with general IT Security relevant information from interest groups and authorities.
- The COS Operation Manager in the development department must stay informed about it-security relevant information from Microsoft around the sources surrounding.

Implementation guidelines

- The IT Security Manager regularly visits the websites below for information:
  https://fe-ddis.dk/CFCS/Pages/cfcs.aspx
  https://www.datatilsynet.dk/forside/
  http://www.digst.dk/
  https://www.cert.dk/
- The Operational-responsible employee in the development department regularly visits the websites below for information:
  https://azure.microsoft.com/en-us/
  https://channel9.msdn.com

6.1.4 IT Security Management

Continia Software's IT Security strategy forms the basis of the company's IT Security and sets the overall framework, primarily focused on Continia Online Services.

The IT Security Manual describes how security is implemented and managed in Continia.

The risk assessment and handling is an ongoing process to ensure continuous updating and development of Continia Software's IT Security Management.

The CEO is responsible for the overall IT Security Strategy and HR, as well as ensuring sufficient staffing and competent resources for other roles in IT Security work.

The IT Security Manager is responsible for management, implementation, systems, follow-up of processes and systems for the IT Security.

The IT Security Committee and other employees with security-related roles are instructed and initiated by the IT Security Manager or the employee's manager.

A central intranet portal has been created for all relevant IT security documents, including this manual, procedure, checklists and incident log, contact information and periodic task management/follow-up.

6.2 MOBILE AND REMOTE JOBS

Employees receive from the company, mobile phones and laptops, which can be used outside the company's network, from which the employee can access the company's internal systems and external hosted systems.

Security measure

- Employees may only use equipment provided by the company for connection, over the internet, to the company's network and externally hosted systems.
- The employee is obligated to treat and store provided mobile equipment with care and common sense to avoid IT Security Vulnerability.
- We have opened access for our employee to access the various online services from outside the Continia Network. Besides User/password policy, VPN, Remote Desktop and SSL communications, we have not implemented any other security measures to secure these devices and their user access.
- On internal networks, only access to authenticated devices is granted.

Implementation guidelines

- When hired, all employees are instructed on IT Security Rules including the use of equipment for connection and sensible care about storing IT equipment outside the company address.
- Our IT security policy states that our employees should primarily access Continia Online Services via internal Server and PCs and only in emergencies use mobile devices/external networks and only through VPN/SSL.

7 EMPLOYEE SAFETY

7.1 EMPLOYMENT

All aspects of the employment, including termination, penalties for breach of contract and confidentiality of company and customers information, are specified in each employee's individual employment contract.

Upon termination of employment, we have a detailed procedure to ensure that a terminated employee returns all company assets in his/her possession, including laptops and mobile devices, as well as to ensure that the employee's access to buildings, systems and data is deactivated. The overall responsibility for securing the completion of the off-boarding process lies with HR.

Security measure

- New employee is checked with a minimum of two external references prior to recruitment.
- Employment contracts contain a confidentiality clause.
- Annual employee review meeting with nearest manager.
- Check list to ensure return of all relevant material and deactivation of system access when an employee off-board.

Implementation guidelines

- Documentation/reference is saved in a dedicated HR System.
- Signed standard contract is saved in a dedicated HR System.
- Annual employee review meeting minutes is saved in dedicated HR System.
- At recruitment or termination, HR distribute and manage the task related to either on-boarding or off-boarding.
- Changes in employment relationships are added as an appendix to the employment contract and is saved in a dedicated HR System.
- The offboarding checklist is evaluated for relevance by the nearest manager of the employee offboarding and completed/performed by HR and is saved in a dedicated HR System.
- When hiring new employees, the employee is made aware of the IT security policy and the IT Security Manual.
- Once a year all employees are briefed about the IT Security strategy.
- In the event of a violation of IT Security's instructions/rules, the employee is reprimanded by the Company, the employment is terminated in the event of repeated violations.

Comments

- The HR system in service is access right restricted, meaning that HR and the CEO has access to all, while other managers only have access to the data for the employees they manage. The individual employee also has access, though only to their own data, and cannot edit anything in the system.

7.2 EDUCATION AND TRAINING

Our assets are very much our employees and we have a structured methodology in relation to the qualifications, training and certifications of our employees.

The employees' qualifications, training and certifications are logged by HR in connection with their hiring and the continuous training.

Security measure

- Employees, where relevant, are informed about our safety guidelines on a regular basis, as well as when changes occur and Continia will continuously assess the need for training.
- In the annual employee review meeting with the nearest manager, the need for training in relation to IT-security is discussed.

Implementation guidelines

- Annual employee review meeting minutes is saved in a dedicated HR System .
- The employee's qualifications are updated at least after the annual employee review meeting.

Comments

- Input to the change of security guidelines will come on an ad-hoc basis, originate from many different persons and channels, and will appear during the continuous risk assessment. Therefore the company encourages all its employees seek relevant information and inform the IT Security committee of potential risks.

8 INFORMATION-RELATED ASSET MANAGEMENT

8.1 RESPONSIBILITY FOR PHYSICAL ASSETS

There are many Physical Devices in and around Continia's infrastructure and with different relevance to IT Security and Online Services. The devices can be categorized into 4 group:

Hosted/Cloud Servers – machines/services hosted by, or rented from external suppliers, for the operation and development of Continia Online Services.

Internal servers and PCs – machines used by Continia employees to access internal company services. The servers were the internal services are hosted.

Customer devices – i.e. access from customer servers, PCs, Web Browsers, Apps, mobile devices that access Continia Online Services.

Other devices – since Continia Online Services is available over the Internet, in principle it is any physical device connected to the Internet.

The Internal IT manager is responsible for the Internal Servers and PCs.

The responsibility for Hosted/Cloud Servers, Customer Devices, and other devices is directly related to Continia Online Services and therefore the responsibility lies with the COS Operations Manager in the development department .

8.1.1 Hosted/Cloud Servers

Security measure

- External suppliers are assessed on physical security in the assessment of external suppliers and partners.
- External suppliers should at least be ISO27001 Certified.
- Hosted/Cloud devices can only be accessed by developers, operations manager and Hosted/Cloud Server administrator.
- Annual tests are performed to tests for vulnerabilities and unwanted intrusion.

Implementation guidelines

- Service contracts with external suppliers are checked and assessed for physical security on devices and for certifications.
- External supplied services must at least comply with internal Domain Security Policy.
- Access takes place only via Internal Continia servers and Continia PCs.
- An penetration/hacker test is executed which is evaluated and appropriate actions are initiated.

8.1.2 Internal servers and PCs

Security measure

- All devices are centrally registered and de-registered.
- All devices are installed with Windows connected to Continia domain and associated windows user.
- All devices are installed with anti-virus and automatic updating.
- Ensure that all data on devices is deleted before disposal.

Implementation guidelines

- Internal IT manager arranges for purchase, installation, user setup and registration for domain, this is logged in the IT Security portal.
- Internal IT manager checks monthly for whether automatic anti-virus update works on all devices and this is logged in the IT Security portal.
- Internal IT manager de-register devices and disable user after instruction from HR or when replacing devices.
- When disposing internal servers and PCs, The Internal IT Manager will remove all data from devices.

8.1.3 Customer devices

Security measure

- Customer devices can only access Continia Online Services using secure password assigned by Continia or using users/password defined by the customer himself.
- Customer devices can only access Continia Online Services via Continia defined Internet addresses and ports.
- External devices that have abnormal or high access/access to Continia Online Services are monitored.

Implementation guidelines

- Monitoring and analysis of external IP addresses, automatic email alert to Operational-responsible employee for abnormal/high activity.

8.1.4 Other devices

Security measure

- General monitoring for unauthorized/destructive devices.
- Check Continia employee does not use other devices to access Continia Online Services.

Implementation guidelines

- External devices that have abnormal or high access/access to Continia Online Services are monitored.

8.2 CLASSIFICATION OF DATA

In order to be able to distinguish between different types of data, who the data relate to and how we treat the data. Data is broken down by customer/users and classified into master data, operational data and transaction data.

Master data is information about the customer such as CVR.nr, name, address, users, and licensing relationships. Master data is stored as documentation and history.

Operational data is information collected to support billing and customer support – such as logs, usage data, session data and login information. Operational data is only stored to the extent necessary for online services and support. Any consumption data is stored as a billing basis and is treated as master data and anonymized after terminated customer relationships.

Transaction data is data which is sent/saved to the online service for example, invoice document, payment authorization and travel settlement. Transaction data is stored by the customer in the online service and is automatically deleted automatically after use.

The overall responsibility for data security lies with the COS Operations Manager.

8.2.1 Master data

Security measure

- Master data is stored only in one place, we do not have the same information stored in several different ways.
- In connection with the purchase of Continia Software, the customer accepts Continia's license terms and hereby grant Continia the right to store data, this acceptance must be recorded with date and user identification.
- Backup is continuously taken so that master data can be restored with 15 minutes interval within the last 14 days and daily within the last 1 year back.
- Master data is backed up to external location daily.
- It must be possible to provide accurate information about what data is stored around a given customer.
- It shall be possible to delete personally identifiable data within 72 hours. However, backup media/file will contain personally identifiable data which is deleted when the backup file is deleted/overwritten. In connection with the restore procedure, personally identifiable data previously deleted in the operation system will be deleted.

Implementation guidelines

- All data is stored in Microsoft Azure SQL Server with associated security measures and user access only for relevant employees.
- All applications with access to data are tested before being put into production.
- Backup and Recovery are tested at least once a year.

8.2.2 Operational data

Security measure

- Operational data is stored only in one location.
- Backups are made daily to secure logs to help with troubleshooting.
- Backup can be restored for up to 1 year.
- Operational data is continuously deleted when they are no longer relevant.
- At the end of customer relationships, all operational data may be anonymized for a given customer upon request from customer.

Implementation guidelines

- Data deletion is monitored.
- Backup and Recovery are tested at least once a year.

8.2.3 Transaction data

Security measure

- Transaction data is created and deleted when the customer initiated an action to upload and is deleted when the customer initiate a download action or after processing.
- Transaction data is stored only in one place.
- Backups are made daily secure restore logs to help with troubleshooting.
- Backup can be restored for up to 1 year.

- It must be possible to provide accurate information about what data is stored around a given customer.
- At the end of customer relationships, all operational data can be deleted for a given customer upon request from customer.

Implementation guidelines

- Transaction data creation and deletion is monitored.
- Backup and Recovery are tested at least once a year.

9 ACCESS MANAGEMENT

9.1 BUSINESS REQUIREMENTS FOR ACCESS MANAGEMENT

9.1.1 Customer Access - License Terms

We have license terms with all our customers which describes the conditions of how to use and access the Continia products, including Continia's Online Services. Changes to these terms will be published and existing customers will be notified about these.

Security measure

- License Terms are the sole agreement that describes the delivery obligations between Continia and the Customer.
- License terms must be presented to and accepted by the customer before commissioning the solution.
- Customer acceptance of the terms must be saved as proof with date and "signer".
- Delivery obligations in the license terms must be assessed each time the delivery conditions of the solution themselves change.

Implementation guidelines

- Requirements for changes to delivery conditions in license terms will come from different origins internally as well as externally – these are collected and assessed on an ongoing basis by the IT Security Committee.
- In regards with upgrading/modifying the solution, the Operations Responsible employee in the development department will check compliance between new solution and delivery conditions in license terms (Deployment Checklist).
- Changes to existing license terms are prepared by the IT Security Committee.
- At a minimum, customers should accept new (modified) license terms when switching version/upgrade.

Comments

- A log should be stored on different versions of license terms and what terms which customers have accepted.

9.2 EMPLOYEE ACCESS - CREATION AND REMOVAL

Employees who have access to the internal Continia network and the users who have access to the external hosted servers/services.

Security measure

- All users must be personally identifiable, i.e. they must be marked with a personal name.
- Users are deactivated after referral from HR.

Implementation guidelines

- Internal IT performs user creation and compliance measures in regard to personal identifiability.

- Internal IT does not delete users but they deactivate users on a given date based on information from HR.

9.2.1 Password

Security measure

- All users in the Continia environment have password restrictions.
- All users have a password and it is systemically set up so that there are limitations to the configuration of the password.
- Passwords be complex, and must adhere to system implemented policy.
- Our employees' password is personal, and only the user him/herself may know the password.

Implementation guidelines

- Only the Administrator-user has permissions to user creation/control/removal.
- Only Operations Responsible employee and CEO has the password to administrator-user.
- Only the employee in the development department has access to COS Hosted/Cloud servers.
- Passwords are Required to meet the Microsoft complexity requirements policy, however with 12 characters minimum length and 12 months maximum age.
- All users in the Continia environment have restrictions regarding access to only relevant parts of the solution.

9.2.2 Review of users

Twice a year, management reviews a list of users created and their access level to ensure that unauthorized persons does not get access.

9.2.3 User access to data

Our employees are set up with differentiated access, and thus only have access to systems and data that is relevant for their work function. Access to systems/data is approved by the employee's nearest manager and the responsible (Internal IT or COS Operations Responsible employee).

9.2.4 Screen lock

We have, where possible, timed out sessions, for instance on applications, databases, servers etc.

9.3 ACCESS ROUTES TO THE OPERATIONAL ENVIRONMENT AND SERVICES

Our online services are complex with many services and data, and to ensure against unauthorized access, and to ensure the transparency of the structure, we have drawn up a number of documents describing the internal components, units, logical network division, etc. These documents and other relevant material are regularly updated by changes and reviewed at least annually by our infrastructure specialists.

The services and operations of the environment can generally be accessed in the following ways:

1. Via web browser and Microsoft user interface for developers and operators with employee user login.
2. From the Microsoft development tool Visual Studio with employee user login.
3. SQL Server Management Studio via user login.

4. Online Services via customer login ie. unique customer address/customer login key/customer user/password.

Security measure

- Employee user has own personal login with complex password rules and limited but relevant access rights.
- Customer access is limited to their own data and access address.
- Our IT security policy states that our employee may only use internal secure devices for access to operational environment.

Implementation guidelines

- Only the Operations Responsible employee and the CEO have Administrator rights.
- Only the Operations Responsible employee can change the operating environment.
- Customer data is kept separate and uniquely identified per customer.
- Customer access is monitored for irregularities.

9.3.1 Accessibility (login, vpn, 2-way, SMS, HTTPS)

Only authorized persons must be able to access to our operational environment, and thus potentially to services and data. Access outside our internal network must only occur in case of emergency. It is possible to log in via encrypted VPN connection. In addition, users have access to cloud services via HTTPS.

9.4 PASSWORD MANAGEMENT

Passwords are controlled by Windows and Hosted/Cloud servers' access (Azure AD).

Security measure

- Utilizes Windows/domain to ensure password complexity and periodic switching.
- Azure AD with access to Hosted/Cloud servers is checked by the Operations Responsible employee before access is granted, as well as on an ongoing basis, at the minimum annually.
- Our IT security policy describes that our employees' password is personal, and only the user him/herself may know the password.

Implementation guidelines

- Internal IT Responsible creates Windows users with the correct user profile settings.

As we have system users, such as service accounts and similar, that cannot be used for login, and for operational reasons do not change passwords on. Such passwords are stored in a password manager in encrypted form. Only the Administrator and the CEO have access to the system. Requirements for these passwords are tougher than our regular password policy.

10 CRYPTOGRAPHY

Continia Software applies encryption to secure data and operation where it makes sense.

Security measure

- Password storage is always stored encrypted
- Communication over public networks to and from Continia Online Services always uses encryption

Implementation guidelines

- Generic user passwords is not saved by Continia itself, instead it is saved at Windows/AzureAD password handling.
- All communications between Continia networks and Azure/Continia Online Services are via HTTPS/SSL.
- All communication between devices outside Continia and the Continia network is conducted through VPN.
- All communication between Continia Online Services and customers is done by means of HTTPS.

11 PHYSICAL SECURITY

11.1 OFFICES/ACCESS

Continia have office facilities in four different locations, spread over three countries.

In Aalborg, Denmark the office, placed on the fourth floor of a larger office and storage complex, is accessed through a manned reception during business hours, all entry points are locked as employees in Aalborg access the office through the use of key tag which are supplied by the office landlord. Outside of normal business hours the office building can only be accessed by the use of the key tag in combination with a password. Both the office and the wider building is fitted with an alarm system, which is activated by intrusion.

In Copenhagen, Denmark the office is placed on the first floor of an office building, the employees must use a key tag to access the office, an alarm system is also fitted to the office.

In Mechelen, Belgium the office is situated on the top floor of 60-meter office building, the floor where the office is situated has a manned reception in which all visitors must register at the reception before being allowed access to the floor. The employees must use a key tag in order to move around the different floors of building for instance when using the lift, this tag must also be used if an employee wishes to enter the building outside of opening hours. Finally, the individual offices are locked, with only the employees having a key to those rooms. The office facilities are also supplied with an alarm system, which is activated by intrusion.

In Blaricum, the Netherlands the employees must use a key to access the office, an alarm system is also fitted to the building, finally the entrance door to the office is under camera surveillance.

Our employees have the option to work from home and we have a policy for the use of company equipment (portable, etc.).

Continia Online services/servers are exclusively located in Microsoft Azure data centers.

The physical security of sub suppliers has been evaluated as part of our annual supplier evaluation.

12 MANAGEMENT OF SERVICES AND OPERATIONAL SECURITY

12.1 OPERATION

We want to ensure that we have a stable, correct and secure operation of our Online Services. The tasks are assigned, delegated, and we ensure this through applying procedures for operational control and change management. Our documentation and processes in general ensure that we exclude or minimize key personnel.

12.1.1 Operating procedure

Security measure

- The operation of Continia Online Services is continuously monitored for errors in performance, security and application.
- The operation of Continia Online Services is implemented with failover support, to handle data center crashes or breakdowns of internet connection to data centers.
- The operation and maintenance of Continia Online Services in the operating environment can only be accessed by Operations Responsible employees.
- All changes to the operating solution should be deployed through a central service, which enables rollback.

Implementation guidelines

- Implementation of monitoring solution - with email notifications in case of irregularities.
- Evaluation and implementation of third party solution over the next 12 months.
- Live Online Services is implemented on Azure in North Europe with the failover option in Western Europe. For customers in US and Asia we are also setting up Online Services in their local data centers for their processing and data storage.
- Only Operations Responsible employees in the development department have access to Azure operating environment.
- Azure DevOps is used for deployment and keeping track of deployment history.

12.1.2 Change management

We have defined a change management process to ensure that changes occur without undue disruption to operations.

Security measure

- Development, Test and Operating environment kept separate
- Regardless of the change in the operating environment, it is always ensured, at least;
    - All changes are approved before commissioning by the Solution Manager and Operations Responsible employee .
    - The system documentation is updated with the new change.

Implementation guidelines

- All changes are described and documented in the development system
- Changes are developed locally at the developer, code is stored in the development system

- Deployment for testing and test of changes is carried out by the relevant employees.
- Deployment to operating environment is approved by the relevant employee and performed by the Operations Responsible employee in the development department.
- Test & Deployment documentation is updated in development system.

12.2 MALWARE PROTECTION

We have implemented scanning and monitoring systems to protect against known harmful code, i.e. what we and our customers— through our platforms — may be infected with on the Internet.

Security measure

- We have antivirus systems on all our Windows devices.
- We have systems for monitoring Internet usage, hardware resource use and traffic, security precautions in other technical and central installations.

Implementation guidelines

- All Windows devices (internal and hosted) are installed with the Windows Virus & Threat Protection anti-virusprogram with automatic program/antivirus database update, and the Internal IT manager is notified if automatic updating is not performed weekly.
- Hosted operation servers on Azure have their security and performance monitored with Azure Security Center, which notifies the Operations Responsible employee in the development department for irregularities.

12.3 BACKUP/FAILOVER OF OPERATING ENVIRONMENT

We ensure that systems and data are restored in an appropriate and correct manner.

Security measure

- The operating platform is run on a redundant environment with a failover warranty from Microsoft.
- Backup to remote location of relevant data is taken (see section on 8.2) (A backup procedure is designed with differentiation on data incl. COS Billing Data – in Billing Project) – Product Manager must assess whether the normal 14 day point-in-time restore functionality we have in SQL today.
- Recovery functionality is tested at least once a year mirroring the operating environment (desktop test).

Implementation guidelines

- An Operations Responsible employee in the development department ensures that the backup has been made, take the necessary measures if the job has failed, and then log this in the operations log.
- An Operations Responsible employee in the development department performs recovery tests at least once a year and logs this in the Operations log. The recovery test must be performed for one product at least, including database restore. Time spent on the task is added to the log to provide an estimate for future execution of the task.

12.4 Logging and Auditing

To ensure documentation of stable operation, data compliance and rapid recovery/troubleshooting, logging and monitoring is necessary.

Security measure

- The operating platform is implemented with automatic monitoring of security attacks and errors and notification for irregularities.
- The operating platform is implemented with logging of usage (login/resources) and system generated messages in connection with security and errors.
- All changes and documentation concerning Continia Online Services are logged.

Implementation guidelines

- The operating platform is implemented with automatic logging and monitoring, and notification to the Operations Responsible employee in the development department.
- The operations officer in the development department is responsible for logging all events and documentation in the central task system.

12.4.1 Capacity and system testing

Time limits are set for performance expectations and performance tests are performed in case of major changes to the solution.

Security measure

- The operating platform is implemented with automatic monitoring and logging of performance and notification in case of deviations from limit values.
- Solution Manager monitors customer experience and performance feedback for each of their products in Continia Online Services.

Implementation guidelines

- The operating platform is implemented with automatic monitoring and notification in case of irregularities.
- In the case of major changes to Online Services, performance tests are performed on a live environment with what is assessed to impact performance.
- Solution Manager has weekly meetings with hotline support staff where any performance related inquiries from customers are processed.

12.5 Operation software

Security measure

- Always Updated Operating System and Operating System Services
- Always Updated Web Server and SQL Server
- Always updated anti-virus

Implementation guidelines

- Windows Update must be set up on all personal computers and servers to automatically download and install updates for all Microsoft products, such as Microsoft. Windows, Office, etc.
- Automatic Anti-virus update of Microsoft Virus & Threat Protection antivirus.
- Windows configured for automatic update (Internal IT manager)

13 COMMUNICATION SECURITY

13.1 NETWORK SECURITY

The IT security around our operating environment and the external frames of data is networked against the Internet, remote or similar. We believe that we have secured data and systems also inside the network, but the external protection against unauthorised access is of our highest priority.

We have set up surveillance and logging of network traffic, and our development department is monitoring this. We do not proactively monitor logged events, but we follow up if we suspect that an incident may relate to matters uncovered in the log.

Access to our operating environment from external devices, is done via encrypted HTTPS access

Only authenticated network traffic (incoming) is allowed through our firewall.

We are responsible for the operation and security ourselves i.e. from and with the services provided by us that extends to the Internet. Our customers are responsible for accessing the Internet.

13.2 INFORMATION TRANSFER

External data communication between services and the customer is done exclusively through Continia defined interfaces and protocols.

First-time passwords for services are sent via email, but these must be changed at first login.

14 Development and Maintenance of Online Services

Design and development of services is performed by employees in the development department. Design and function changes are assessed in relation to security policy and any necessary changes in policy and controls are updated.

Development and testing are carried out in a development environment where tests of functionality, data, stability and security are completed satisfactorily before new developments are declared ready for release.

14.1 Development/Design Safety Requirements

Security measure

- Design is verified for compliance with license agreement, data protection legislation and IT Security Strategy.
- Designed according to Best Pratices design for Microsoft technology platform.

Implementation guidelines

- Design is subject to collaboration between Solution Manager and Developer.
- The developer designs details and implement/codes.

14.2 Security in development process

Security measure

- Always use Azure DevOps, SourceControl, or BitBucket, where new development is made on a daily basis.
- External components are virus scanned and their authenticity is verified/evaluated by the application of common sense.
- Periodic code review of colleagues' code.

Implementation guidelines

- Azure DevOps enforces code review on all committed code.

14.3 Test

Security measure

- Test plan is prepared and executed within commissioning.
- Test plan should include at least a test of the primary functions.
- Test data does not leave Continia's systems.
- Employee has knowledge about test data and test results.

Implementation guidelines

- The Solution Manager is responsible for test cases and test execution.
- Employee contracts require employees to ensure confidentiality about customer relationships/data and internal company information (test results).

15 SUBCONTRACTORS

15.1 EXTERNAL SUPPLIERS

Continia's Online Services are critical to many customers worldwide, subcontractors that provide services to Continia Online Services, should therefore at least meet the same IT security requirements/standards as Continia itself and generally be larger and financially solid companies. This is to ensure the stability and security of the subcontractor's services, also in the longer term.

Continia develops and operates our solutions on Microsoft technology and services, and Continia will to the extent possible use the opportunities that Microsoft provides for operational and data security. Microsoft cloud services are compliance certified and these certifications are assessed on an ongoing and regular basis.

15.2 COOPERATION WITH EXTERNAL SUPPLIERS

Where we use subcontractors, we supervise the agreed deliveries, as they must comply with our own performance delivery policies, including our business terms with our customers. As a supervision measure we annually receive/check online - an auditor's statement/certification for the agreements entered into by the subcontractors, who either receive such certification or gets a report drafted.

Security measure

- Assessment of service (SLA) and finances of new external suppliers before the start of cooperation.
- Annual assessment of service (SLA) and finances of existing external suppliers.

Implementation guidelines

- Documentation of annual assessments and contracts is stored on the IT Security portal.
- In progress and follow-up of improvement initiatives.
- The IT Security Committee is responsible for assessing external suppliers and partners.

Comments

- The annual supplier assessments also assesses the importance of the different suppliers.

16 MANAGING SECURITY INCIDENTS

16.1 SECURITY INCIDENT REPORTING

Security incidents are reported and documented in our internal task system. In this we can escalate the rating, so that some tasks are given higher priority than others. In addition, security incidents resulting from respectively, observations made be employees, alerting from the log and monitoring system, telephone inquiries from customers, subcontractors or business partners, will be escalated from our hotline with simultaneous information provided to management.

Our business partners and customers are obliged, through the contracts and agreements entered into, to report any security incident, so that the incident can be reacted to as soon as possible and necessary actions can be taken through established procedures.

Security measure

- All security incidents are logged, prioritized, and handling documented.
- Reporting a security incident notifies the Operations Responsible employee.
- All employees are encouraged and informed about how to report any security incident.

Implementation guidelines

- In the event of a security incident, an email is submitted to cotask@continia.com and with tl@continia.com in CC (Continia Online Service operations manager).
- A task is automatically created in the internal task system and the task is assigned to the Operations Responsible employee, who is also notified by mail.
- The security incidents can be prioritized with Outlook's Priority feature:
    - High - Critical for operation or data security that should be handled immediately.
    - Normal - Incident that should be handled among ordinary work tasks.
    - Low - Incident that should be handled at the next release/update.
- At hiring and at the annual security update employees are informed about the reporting process.

16.2 MANAGING SECURITY INCIDENTS

If an incident occurs outside normal working hours, it is the individual employee who assesses what action is appropriate. The necessary briefing is then performed to inform customers and other external stakeholder, and to remedy the relationship.

This is occurs after consultation with management or colleagues.

If an incident occurs during normal working hours, the development department will handle and escalate the case in the same way as other cases along with prioritization that is deemed necessary. For management and control of monitoring purposes, as well as follow-up of incidents, our log system is used for registering, prioritization, and escalation of incidents. The process is documented in our log system.

Security measure

- All security incidents are logged, prioritized, and the handling documented.

- The Operations Responsible employee can delegate, prioritize, and follow up on tasks related to security incidents.
- The Operations Responsible employee can escalate critical security incidents to the CEO to ensure adequate attention and resource allocation from relevant parts of the organization.

Implementation guidelines

- The Operations Responsible employee must for all security incidents, assess and initiate activities, all of which are recorded and followed in the internal task system
- Security incidents are assessed based on the impact/risk on the operation of Continia Online Services and security concerning customer data. A plan is drafted for the management of the security incident.
- In the context of the assessment of the scope/impact of a security incident, resources are allocated for further analysis/investigation and repair.

16.3 Evaluation of security incidents

A security incident may, depending on the relationship, be the subject of subsequent investigation. This can occur internally for the purpose of evaluation and possible changes in procedures, technical or logical conditions. It is also a possibility that there will be a police investigation if the incident has criminal element to it. In all cases, our logging and other monitoring systems will be able to be used to evaluate the security incident.

Security measure

- All security incidents are evaluated after they are handled.
- In addition to the evaluation, we conduct a root cause analysis to ensure that the security incidents that occur do not recur.

Implementation guidelines

- Before the handling of a security incident can be completed, an evaluation of the event in the task system must be performed and documented.
- All evaluations shall be reviewed at least at the half-year risk assessment, in the case of critical incidents or incidents where activities must or can be initiated instantaneously, the Operations Responsible employee will initiate these.

17 Contingency management

17.1 Contingency plan

Should an emergency/critical situation arise in or around Continia Online Services, Continia Software A/S has developed a contingency plan. The contingency plan is anchored in the IT risk analysis and is maintained annually at the minimum following the performance of the risk analysis.

Security measure

- Continia requires it staff to be flexible in order to step into sudden emergency situations.
- Only Continia Online Service suppliers that are ISO27001 certified are selected.

- Failover and backup solutions have been established for the rapid restoration of services and data described and known by key employees.
- Monitoring solutions have been implemented to automatically monitor stability and data security.

Implementation guidelines

- All employment contracts carry stipulations of flexible working hours. Employees are offered flexible working hours against the expectation that they are also available in emergency situations.
- Suppliers are checked annually for their certifications by the supplier responsible (Internal IT or COS Operations employees).
- Backup and failover procedures are tested at least once a year and any changes are logged and recovery procedures are updated.

The plan is continuously assessed as part of our contingency efforts, so that we ensure that customers will experience a minimum of disruption to their operation if an emergency situation occurs.

18 COMPLIANCE WITH LEGAL AND CONTRACTUAL REQUIREMENTS

According to Danish law, Continia is subject to the Danish Data Protection Act as a data processor for the personal data we may store/transport in our solutions as well as the Marketing Act with respect to the data processing and marketing based on these data.

Continia is also obligated by the license agreement between the customer/user of Continia products and Continia Software A/S.

EU General Data Protection GDPR, strengthens the requirements for the handling of personal data and the adjoining procedures, this legislation officially entered into force in Denmark on 25 May 2018. Continia's goal is to comply with this legislation at any time.

We allow ourselves annually to be audited by the external auditor for the purpose of providing a declaration of compliance with the controls mentioned in this description.

19 AUDIT LOG

Review	Change description	Date/Author	Changes:
0.9	Initial presentation for the Information Security Handbook	2016/11/1 - Torben Kragelund	
4.1	Updated for 2018, including GDPR	2017/11/28	GDPR + ref. For CSF
4.3	Updated with access authentication requirements	2018/1/12 – Torben Kragelund	9.2
4.5	2019 Review Update	2019/3/1 - Torben Kragelund	
5.0	2020 Review Update	2020/4/1 – Torben Kragelund	Translation & Minor adjustments

20 APPENDIX

20.1 APPENDIX A - CONTINIA SOFTWARE LICENSE TERMS

Insert here.

20.2 APPENDIX B – DATA PROCESSING AGREEMENT

Reference to relevant paragraphs: