Common IT Security Controls questions Visma.net Payroll public SaaS

	Control Category	IT Security Control Text	Control Answer	Comment
1.1 User authentication	1 Access Control	5. Encrypt or hash with a salt all authentication credentials when stored	Yes	
1.1 User authentication	1 Access Control	3. The authentication token or account is possible to revoke	Yes	
1.1 User authentication	1 Access Control	1. User is authenticated during sign-on procedure	Yes	
1.1 User authentication	1 Access Control	9. Periodic reauthentication of authenticated sessions is performed every 12 hours or 30 minutes inactivity; may use one authentication factor	Yes	
1.1 User authentication	1 Access Control	8. Multi-factor authentication mechanism is used, AAL2	Yes	
1.1 User authentication	1 Access Control	4. The authentication process is protected against modification and unauthorized usage during transmission	Yes	
1.1 User authentication	1 Access Control	2. Re-authentication is done if the session has timed-out	Yes	
1.2 Sign-on procedure	1 Access Control	1. No system or application identifiers are displayed until the sign-on process has successfully been completed	Yes	
1.2 Sign-on procedure	1 Access Control	5. Additional sign-on attempts are restricted	Yes	
1.2 Sign-on procedure	1 Access Control	7. Credentials are protected in transit	Yes	
1.2 Sign-on procedure	1 Access Control	4. The duration of a sign-on procedure is limited	Yes	
1.2 Sign-on procedure	1 Access Control	3. The numbers of unsuccessful sign-on attempts are limited (e.g. a re-try limit of three attempts in a 24-hour period before disabling the user account for a predefined period of time)?	Yes	
1.3 Sign-off procedure	1 Access Control	1. The sign-on procedure is required again following a sign-off from the application	Yes	
1.3 Sign-off procedure	1 Access Control	2. When a session is ended, the session is terminated and its data is deleted	Yes	
1.4 User Authorization	1 Access Control	2. There is an approved process for authorizing users, which assign users with default access based on the principle of least privilege (e.g. ‘none’ rather than ‘read’)	Yes	
1.4 User Authorization	1 Access Control	3. User authorization is based on role, rule or attribute-based access control	Yes	
1.4 User Authorization	1 Access Control	1. There is an approved process for authorizing users, which associate access privileges with defined users (e.g. using unique identifiers such as User IDs) to provide individual accountability	Yes	

1.5 Session handling	1 Access Control	1. Ensure Session IDs cannot be easily predicted (e.g. by using randomly generated Session IDs)	Yes	
1.5 Session handling	1 Access Control	7. A new session is established after authentication (mitigating session fixation attack)	Yes	
1.5 Session handling	1 Access Control	6. The old session is invalidated prior to authentication	No	System allows multiple active sessions by same account across browsers and devices
1.5 Session handling	1 Access Control	2. The session is limited in time	Yes	
1.5 Session handling	1 Access Control	4. Configuring the security parameters in cookies used to hold session information, e.g. HTTPOnly, Secure, etc. For Web applications only	Yes	
1.5 Session handling	1 Access Control	5. The session is unique per user	Yes	
1.5 Session handling	1 Access Control	3. Inactive sessions are shut down or reauthenticated after a defined period of inactivity	Yes	
2.1 Input Data Validation	2 Application Intrusion Protection	2.The application is placed in front of an application firewall to verify and validate the traffic going to the application. Any unauthorized traffic should be blocked and logged. For web applications only.	Yes	Session/Cookie is validated
2.1 Input Data Validation	2 Application Intrusion Protection	1. Data/information input in applications is validated by using range, size, type, consistency, comparison, validity and boundary checks	Yes	Various checks
2.2 Output Data Validation	2 Application Intrusion Protection	2. The output data is encoded (use of escaping) to ensure that characters are treated as data and is not intended to be executed. For Web applications only	Yes	By each service
2.2 Output Data Validation	2 Application Intrusion Protection	1. Data/information output from applications is validated by using range, size, type, consistency, comparison, validity and boundary checks	Yes	By each service
2.3 Communication Protection	2 Application Intrusion Protection	1. Transmitted confidential information is protected against unauthorized disclosure (confidentiality) in external connections	Yes	
2.5 Tamper Protection	2 Application Intrusion Protection	2. Digital signatures of customer agreements, contracts, messages or similar are used in the solution, to enable the identity of the originator?	Yes	
2.5 Tamper Protection	2 Application Intrusion Protection	1. Transmitted confidential information is protected against unauthorized manipulation (integrity) in external connections	Yes	
2.6 Information leakage protection	2 Application Intrusion Protection	2. Error messages or other failures such as authentication or authorization failures that contain sensitive information are limited when displaying to users	Yes	
2.6 Information leakage protection	2 Application Intrusion Protection	1. Sensitive comments in client code are removed before production	Yes	By each service

2.7 Error and Exception Handling	2 Application Intrusion Protection	1. When an unexpected error or failure in the application occurs, the error is reported and a secure state is maintained	Yes	
3.1 Security Event Logging	3 Security Event Logging	2. The user identity is registered in every event	Yes	
3.1 Security Event Logging	3 Security Event Logging	4. Creation of new identities and roles are registered	Yes	
3.1 Security Event Logging	3 Security Event Logging	3. Failed authentications are registered	Yes	
3.1 Security Event Logging	3 Security Event Logging	1. Date and time are registered for every event	Yes	
3.1 Security Event Logging	3 Security Event Logging	5. Changes on current access rights are registered	Yes	
3.2 Management of Security Log	3 Security Event Logging	4. Security logs are backed-up for 15 months	Yes	
3.2 Management of Security Log	3 Security Event Logging	3. Entries in the security log are not overwritten or deleted before archiving is done	Yes	
3.2 Management of Security Log	3 Security Event Logging	1. Management of security log is protected by access control	Yes	
3.2 Management of Security Log	3 Security Event Logging	2. Entries in the security log are not able to be tampered with	Yes	
3.2 Management of Security Log	3 Security Event Logging	5. Logs must be integrity protected in transit	Yes	
4.1 User identification	4 Identity and Access Control Management	2. The unique user id is not reused over time	Yes	
4.1 User identification	4 Identity and Access Control Management	1. The system uses a unique user id (SID)	Yes	
4.2 User and Application Access Management	4 Identity and Access Control Management	6. The application(s) access management is centrally managed	Yes	
4.2 User and Application Access Management	4 Identity and Access Control Management	5. All approvals and authorization requests are traceable to individuals	Yes	
4.2 User and Application Access Management	4 Identity and Access Control Management	7. Privileged users are controlled. See section “Privileged Access Management”	Yes	
4.2 User and Application Access Management	4 Identity and Access Control Management	3. The management of user identities and access rights are protected by access control	Yes	
4.2 User and Application Access Management	4 Identity and Access Control Management	8. User and application access rights are reviewed at least semi-annually	Yes	Yes, from a devops perspective. From a user perspective this is handled by the customer.
4.2 User and Application Access Management	4 Identity and Access Control Management	4. All non-personal accounts (e.g. service, system, robot, root accounts) must have an appointed and documented owner, preferable assign ownership to a role rather than a person	Yes	This is documented in our management system and assign to administrative roles
4.2 User and Application Access Management	4 Identity and Access Control Management	1. Requests for granting, altering or removal of users' access rights are approved by appropriate role	Yes	
4.2 User and Application Access Management	4 Identity and Access Control Management	2. There are procedures for granting, altering and removing access privileges	Yes	
4.3 Privileged Access Management	4 Identity and Access Control Management	4. The checkouts of actions are to be reviewed on a monthly basis and privileged users are to be reviewed semi-annually	Yes	

4.3 Privileged Access Management	4 Identity and Access Control Management	3. Ensure that all temporary access in production is traceable to a documented change request or equivalent request	Yes	
4.3 Privileged Access Management	4 Identity and Access Control Management	1. Ensure that only authorized users have write access to the applications production environments	Yes	
4.3 Privileged Access Management	4 Identity and Access Control Management	2. Ensure that only temporary access rights shall be granted	Yes	
5.1 Application Hardening	5 Application Threat and Vulnerability Management	1. All unnecessary services and functions in the application or system are removed	Yes	
5.1 Application Hardening	5 Application Threat and Vulnerability Management	2. Configurations supplied by vendors are configured securely according to recommendations from the vendor or from best practices, e.g. change default password settings.	Yes	
5.2 Security Patch Management	5 Application Threat and Vulnerability Management	2. Security patch routines are in place to make sure that latest patches are updated into the application	Yes	Continuesly
5.2 Security Patch Management	5 Application Threat and Vulnerability Management	3. Patches are tested before deployment	Yes	
5.2 Security Patch Management	5 Application Threat and Vulnerability Management	1. The version of the installed application is documented	No	We perform continuesly development and releases, with several releases every day. No specific version. Version control on code of course.
5.3 Application Vulnerability Scanning	5 Application Threat and Vulnerability Management	3. Application Vulnerability Scanning are performed at least monthly or before deployment of a new released application	Yes	Continuesly
5.3 Application Vulnerability Scanning	5 Application Threat and Vulnerability Management	1. Identify known and common technical vulnerabilities by using testing vulnerability scanning tools	Yes	Continuesly
5.3 Application Vulnerability Scanning	5 Application Threat and Vulnerability Management	2. Follow-up and mitigate detected vulnerabilities according to specified remediation priority stated in document "Vulnerability severity rating"	Yes	According to our documentation, not customers.
5.4 Application Security Testing	5 Application Threat and Vulnerability Management	1. Identify known and common technical vulnerabilities by using third party security testing services	Yes	
5.4 Application Security Testing	5 Application Threat and Vulnerability Management	2. Follow-up and mitigate detected vulnerabilities according to specified remediation priority stated in the document "Vulnerability severity rating"	Yes	According to our documentation, not customers.
5.4 Application Security Testing	5 Application Threat and Vulnerability Management	3. Security tests are performed at least annually and/or after major changes.	Yes	
6.1 Protection of source code	6 Application Development Management	2. Access to source code is controlled	Yes	
6.1 Protection of source code	6 Application Development Management	4. Malicious code is prevented from being downloaded into development environments	Yes	
6.1 Protection of source code	6 Application Development Management	3. Version control is applied	Yes	

6.1 Protection of source code	6 Application Development Management	1. All confidential information is removed from the source code	Yes	Source code does not include any customer data.
6.2 Separation of development, test and production environment	6 Application Development Management	3. Different user accounts are used for separating development and acceptance test environments from production environment	Yes	
6.2 Separation of development, test and production environment	6 Application Development Management	4. Physically or logically segregate the production environment	Yes	
6.2 Separation of development, test and production environment	6 Application Development Management	1. The development and acceptance test environments are isolated from the production environment	Yes	
6.2 Separation of development, test and production environment	6 Application Development Management	2. Access to development, acceptance test and production environments are restricted and controlled	Yes	
6.3 Protection of test data	6 Application Development Management	1. Confidential production data (e.g. customer data) is de-identified before using it as test data	Yes	
7.1 Specifications of security requirements	7 Secure Development	4. Security requirements, according to the life cycle of the information handled in the application (including creation, processing, storage, transmission and destruction), are specified	Yes	
7.1 Specifications of security requirements	7 Secure Development	2. Security requirements, when accessing information from particular locations, are specified	Yes	
7.1 Specifications of security requirements	7 Secure Development	1. Security requirements, when accessing information by particular types of users, are specified	Yes	
7.1 Specifications of security requirements	7 Secure Development	3. Security requirements, when accessing particular types of information, are specified	Yes	
7.1 Specifications of security requirements	7 Secure Development	5. Misuse cases are specified to describe abusive scenarios	Yes	Logged by each service
7.2 Secure system design	7 Secure Development	2. Potential threats and missing security controls are considered by conducting ‘threat modelling’ or security design review	Yes	
7.2 Secure system design	7 Secure Development	1. The system design phase involves the use of security architecture principles and security patterns	Yes	
7.3 Secure system build and development	7 Secure Development	5. Ensure that only fully supported web browsers are allowed, ideally only using the latest version of the browsers provided by the vendor. For Web applications only.	Yes	We do not control this for customers environment
7.3 Secure system build and development	7 Secure Development	2. Methods of managing the use of code samples (e.g. defining acceptable sources for developers to obtain sample code and requiring a security review of any sample code before it can be used in the system)	Yes	
7.3 Secure system build and development	7 Secure Development	6. Enable anti-exploitation features such as Data Execution Prevention (DEP) and Address SpaceLayout Randomization (ASLR) that are available in a compiler or operating system configuration settings or deploy appropriate toolkits that can be configured	Yes	Yes, eg enabled out of the box config from AWS

7.3 Secure system build and development	7 Secure Development	7. Security scanning and testing are incorporated in the build process	Yes	
7.3 Secure system build and development	7 Secure Development	3. Secure methods of making changes to the base code of software packages are followed	Yes	
7.3 Secure system build and development	7 Secure Development	4. The build of systems under development is inspected to identify unauthorized modifications or changes, which may compromise security controls	Yes	
7.3 Secure system build and development	7 Secure Development	1. Methods of secure coding best practices and guidelines are followed, e.g. Java Secure Coding guideline, Secure Coding guidelines for .Net, OWASP Secure Coding Practice and OWASP Cheat Sheet series	Yes	
7.4 Security testing	7 Secure Development	3. Test cases are based on misuse cases	Yes	business continuity plans for all teams
7.4 Security testing	7 Secure Development	8. Manual security code reviews are conducted to ensure and to verify that secure coding techniques are used appropriate for the teams coding languages	Yes	
7.4 Security testing	7 Secure Development	5. Manual security code reviews are conducted to ensure and to verify that the proper security controls are present	Yes	
7.4 Security testing	7 Secure Development	4. Apply static and dynamic analysis (SAST and DAST) tools to verify that secure coding practices are being adhered to for internally developed software	Yes	
7.4 Security testing	7 Secure Development	1. Identify known and common technical vulnerabilities during the development phase by assessing open source software/components (FOSS) and/or other third-party components	Yes	
7.4 Security testing	7 Secure Development	6. Manual security code reviews are conducted to ensure and to verify that the proper security controls work as intended	Yes	
7.4 Security testing	7 Secure Development	7. Manual security code reviews are conducted to ensure and to verify that the proper security controls have been invoked in all the right places	Yes	
7.4 Security testing	7 Secure Development	2. Follow-up and mitigate detected vulnerabilities	Yes	
7.5 Secure deploy	7 Secure Development	1. New systems/functionality should be installed in the production environment in accordance with a documented installation process.	Yes	
7.5 Secure deploy	7 Secure Development	2. Automated process is used for deployment	Yes	
8.1 Application Backup Management	8 Disaster Recovery		Yes	
8.1 Application Backup Management	8 Disaster Recovery	1. Information and software data are backed up	Yes	
8.1 Application Backup Management	8 Disaster Recovery	3. The result of the test is documented	Yes	

8.1 Application Backup Management	8 Disaster Recovery	4. Ensure that backups are properly protected via physical security or encryption when they are stored,as well as when they are moved across the network. This includes remote backups and cloud services	Yes	