zivver

How Zivver Helps Organisations with ISO 27001 Compliance

Solution brief

Table of contents

Introduction

ISO 27001:2013 is the internationally recognised framework for an Information Security Management System (ISMS) which outlines a set of rules to protect the confidentiality, integrity and availability of information within the organisation.

There are 114 ISO 27001:2013 controls organised into 14 sections, numbered from A.5 through to A.18. This document lists the 22 controls covered by the Zivver platform that can help organisations comply with the ISO 27001:2013 standard.

ISO 27001 Control

A.6 Organisation of Information Security

A.6.2 Mobile Devices and Teleworking

Objective: To ensure the security of teleworking and use of mobile devices.

A.6.2.2 Teleworking

A policy and supporting security measures shall be implemented to protect information accessed, processed or stored at teleworking sites.

Zivver can help organisations implement security measures that can be used to protect access to sensitive information by a remote workforce, from any modern browser for computer, laptop, tablet and mobile on any (still supported) operating system. We also have mobile apps for iOS and Android, which can ensure no sensitive data is stored on the device. Our mobile applications can be further protected, after first time authentication, with native mobile features like face recognition and/or fingerprint or pin code if required. The mobile apps can also be deployed via mobile device management tools and we can provide administrators the functionality to invalidate active sessions if a device has been lost/stolen to mitigate any risk.

A.7 Human Resource Security

A.7.2 During Employment

Objective: To ensure that employees and contractors are aware of and fulfil their information security responsibilities.

A.7.2.2 Information Security Awareness. Education & Training

All employees of the organisation and, where relevant, contractors, shall receive appropriate awareness education and training and regular updates in organisational policies and procedures, as relevant for their job function.

Zivver's secure email solution contributes to an organisation's security awareness program by alerting users in real time as they are composing a message, adding attachments to it, or selecting recipients, particularly if it contains sensitive information of a specific category and/or the recipient is possibly incorrect, given the type of content being shared. These caution warnings coach the user on what type of information is sensitive according to an organisation's data security policy and helps prevent sending sensitive information in an unsafe manner, whilst also reducing the likelihood of selecting the wrong recipient.

A.8 Asset management

A.8.2 Information classification

Objective: To ensure that information receives an appropriate level of protection in accordance with its importance to the organisation.

A.8.2.1 Classification of information

Information shall be classified in terms of legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification.

Zivver can be used to classify information in real time and automatically enforces specific security levels for certain types of information.

A.8.2.2 Labeling of information

An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information classification scheme adopted by the organisation.

Zivver's secure email solution will automatically label the content of the message and its attachments, while applying the associated security levels indicated in the classification scheme.

A.9 Access Control

A.9.2 User Access Management

Objective: To ensure authorised user access and to prevent unauthorised access to systems and services.

A.9.2.2 User Access Provisioning

A formal user access provisioning process shall be implemented to assign or revoke access rights for all user types to all systems and services.

Zivver supports your formal user access provisioning process by providing the functionality to automatically administer accounts by using our SyncTool. For example when creating accounts for new employees, or updating, blocking and deleting accounts when an employee leaves.

A.9.2.4 Management of Secret Authentication Information of Users

The allocation of secret authentication information shall be controlled through a formal management process.

Zivver supports Single Sign-on (SSO) so that a user can login with their enterprise credentials. Zivver integrates with any identity provider (IdP) that supports SAML 2.0.

A.9.4 System and Application Access Control

Objective: To prevent unauthorised access to systems and applications.

A.9.4.1 Information Access Restriction

Access to information and application system functions shall be restricted in accordance with the access control policy.

Zivver encrypts the contents (message body and attachments) of emails sent with Zivver (Zivver message), where they are transmitted to and stored in our secure cloud using the best-inclass asymmetric encryption. For highly sensitive messages, an additional requirement can be set so recipient(s) of a Zivver message are required to identify themselves via two-factor authentication. That way, you can be certain that the message reaches the correct individual(s). Zivver provides two-factor authentication via a code sent to the recipient mobile phone or two-factor authentication apps (such as Google authenticator). This means only the sender and intended recipient can access the Zivver message. In the event a Zivver message has been sent to the incorrect recipient, Zivver provides features for the sender to instantly revoke the message and view who has opened and/or downloaded attachments.

A.9.4.2 Secure Log-On Procedures

Where required by the access control policy, access to systems and applications shall be controlled by a secure log-on procedure.

Two-factor authentication can be configured for all enterprise Zivver accounts to provide a secure log-on procedure. These accounts can be protected with two-factor authentication via a code sent to the recipient mobile phone or two-factor authentication apps (such as Google authenticator). Zivver also supports Single Sign-on (SSO) so that a user can login with their enterprise credentials, as long as the identity provider (IdP) supports SAML 2.0. Recipients of Zivver messages are also required to identify themselves via two-factor authentication. That way, users are assured that the message reaches the correct individual(s). Zivver provides two-factor authentication via a code sent to the recipient mobile phone, access codes or two-factor authentication apps (such as Google authenticator) when the recipient optionally signs up for a free Zivver account.

A.10 Cryptography

A.10.1 Cryptographic Controls

Objective: To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.

A.10.1.1 Policy on the use of cryptographic controls

A policy on the use of cryptographic controls for protection of information shall be developed and implemented.

Zivver provides cryptographic controls which organisations can use as part of their policy to securely share sensitive information where necessary. All data that is sent to the Zivver servers (Data in Transit) is sent encrypted using TLS 1.2 or higher. Best practice AES encryption is used to store all Zivver messages (Data at Rest).

A.10.1.2 Key Management

A policy on the use, protection and lifetime of cryptographic keys shall be developed and implemented through their whole lifecycle. Zivver's key management policy ensures Zivver never holds the data owner's keys, nor can it give access to third-parties, yielding better data access restraints than Google and Microsoft, for example. This means only the sender and intended recipient can ever access the contents of a Zivver message and the administrative overhead of key management is eliminated.

Administrators have visibility of users who have lost access to messages due to forgetting their password and having to create or request a new one. As Zivver messages are encrypted with a key that is derived from the password of the user account, if the password is reset the user will receive a new key, which no longer decrypts all previously sent messages as they were encrypted with a different key. In situations where this occurs, administrators have visibility of this and are able to rekey all previously sent messages with the new key to restore user access.

A.12 Operational Security

A.12.2 Protection from Malware

Objective: To ensure that information and information processing facilities are protected against malware.

A.12.2.1 Controls against malware

Detection, prevention and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness. Zivver uses an antivirus engine for automatically detecting and blocking trojans, viruses, malware & other malicious threats when attachments are uploaded to Zivver. Users are alerted in real time to make them aware of any issues and also blocked from sending the Zivver message until the malicious attachment has been removed.

A.12.4 Logging and Monitoring

Objective: To record events and generate evidence.

A.12.4.1 Event Logging

Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed.

Administrators are able to view the communication log of a user message, which includes everything related to messages sent with Zivver. Communication logs report on user actions per message e.g uploading attachments, revoke access, recipients opening, downloading or forwarding of messages and if a business rule was triggered. Additional reports can also show how often business rules are ignored and which v erification methods are used.

A.12.4.2 Protection of Log Information

Logging facilities and log information shall be protected against tampering and unauthorised access.

Users are able to view their own individual communication logs which includes everything zivver related to messages sent with Zivver and administrators are able to view all communication logs of users. These logs are protected with two factor authentication access controls and neither admins or users are able to alter or delete logging information.

A.12.4.3 Administrator & Operator Logs

System administrator and system operator activities shall be logged and the logs protected and regularly reviewed.

System Administrator activities such as configuration changes, logging in, changing passwords or changing business rules are logged and available for reporting purposes and audits.

A.13 Communications Security

A.13.2 Information Transfer

Objective: To ensure the protection of information in networks and its supporting information processing facilities.

A.13.2.1 Information Transfer Policies and Procedures

Formal transfer policies, procedures and controls shall be in place to protect the transfer of information through the use of all types of communication facilities.

Zivver's communication platform has many features that help organisations implement controls that can be used to protect the transfer of sensitive information and prevent unauthorised disclosure, also known as a data leak, including, but not limited to:

Before Sending

- Warning users about sensitive information in a message or attached files
- Warning users about unusual recipients, because they have never shared similar information with the recipient before
- Warning users an attached file contains email addresses that differ from the recipient address, suggesting the wrong recipient has been selected
- Warning users that Cc has been selected where Bcc should potentially be used
- Automatically activating security controls based on the content of the message or recipients addressed

During Sending

- Encrypts all information in transit with TLS 1.2 or above
- Stores messages and files at rest using best-in-class encryption without Zivver having access to the decryption keys (Zero-Knowledge Encryption)
- Messages can only be decrypted by a sender and intended recipient(s)

After Sending

- Users and recipients can only access messages after strong authentication
- One Time Passcode via SMS
- TOTP-based authenticator app linked to Zivver account
- Access code
- Verification email
- SSO via SAML 2.0 (for users)
- Instantly revoke messages if a data leak is detected
- Advanced real time logging and analytics to identify risks and impact of (potential) data leaks

A.13.2.3 Electronic Messaging

Information involved in electronic messaging shall be appropriately protected.

Zivver's Secure Email feature works by monitoring the email recipient address, messages and attachments for content containing sensitive information. In the event of a potential threat, Zivver alerts the user with real time visual warnings, in line with your data security policy, that must be addressed before proceeding with sending the email. Even if a mistake has been made after the alert occurs, the Zivver platform provides the ability to instantly revoke a message for any original and forwarded recipients.

All data that is sent to the Zivver servers (Data in Transit) is sent encrypted using TLS 1.2 or higher. Best practice asymmetric encryption is used to store all Zivver messages (Data at Rest). The Zivver platform makes use of zero-knowledge encryption, so Zivver cannot view the content of your messages and attachments. This means only the sender and intended recipient can ever access the contents of a Zivver message.

For highly sensitive messages sent via Zivver, additional requirements can be put in place so that the recipient(s) identify themselves via two-factor authentication. That way, you can be assured that the message reaches the correct recipient(s). Zivver provides two-factor authentication via a one time passcode sent to the recipient(s) mobile phone, access codes or two-factor authentication apps (such as Google Authenticator).

A.14 System Acquisition, Development and Maintenance

A.14.1 Information Transfer

Objective: To ensure that information security is an integral part of information systems across the entire lifecycle. This also includes the requirements for information systems which provide services over public networks.

A.14.1.2 Securing Applications Services on Public Network

Information involved in application services passing over public networks shall be protected from fraudulent activity, contract dispute and unauthorised disclosure and modification. All Zivver messages are encrypted in transit and at rest using best-practice encryption with additional two-factor authentication to access them. TLS 1.2 for in transit encryption protects against eavesdropping and/or modification of content. This guarantees sensitive information is protected from fraudulent activity, unauthorised access or disclosure during transit to the intended recipient(s). Messages sent to the incorrect recipients can be instantly revoked with real time logging and analytics providing insights into potential data leaks, for example, has a message been read and/or attachments been downloaded.

Zivver also supports the implementation of DANE which enables domain administrators to specify the keys used by TLS servers or clients in their domain. This removes the need to depend on third-party certificates attesting the keys are legitimate. Zivver tests for the presence of a TLSA record and of DNSSEC proof.

A.14.1.3 Protecting Application Services Transactions

Information involved in application service transactions shall be protected to prevent incomplete transmission, misrouting, unauthorised message alteration, unauthorised disclosure, unauthorised message duplication or replay.

Zivver's communication platform provides the functionality to help organisations securely send sensitive information from source systems/ applications via out-of-the-box interfaces, to prevent unauthorised disclosure, unauthorised message alteration and misrouting.

A.16 Information Security Incident Management

A.16.1 Management of Information Security Incidents and Improvements

Objective: To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.

A.16.1.7 Collection of Evidence

The organisation shall define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence.

Zivver's audit logging and analytics help organisations identify risks and collect security event related information, giving insights into the impact of (potential) data leaks, which can then be used as evidence.

A.17 Information security aspects of business continuity management

A.17.2 Redundancies

Availability of information processing facilities Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.

Zivver makes sure all messages, attachments and account information are stored redundant in two data centers. Additionally all critical product components are also set up redundantly to ensure that Zivver's secure communication platform meets high availability standards.

A.18 Compliance

A.18.1 Compliance with Legal and Contractual Requirements

Objective: To avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements.

A.18.1.3 Protection of Records

Records shall be protected from loss, destruction, falsification, unauthorised access and unauthorised release, in accordance with legislatory, regulatory, contractual and business requirements.

Zivver ensures all messages are secured and integrity maintained by encrypting them in transit and at rest using best practice encryption, whilst also requiring two-factor authentication to access them protects against unauthorised access. Such features aid in helping organisations comply with the ISO 27001:2013 requirements of this control.

A.18.1.4 Privacy and Protection of Personally identifiable Information

Privacy and protection of personally Widentifiable information shall be ensured as required in relevant legislation and regulation where applicable.

Zivver facilitates the protection of personally identifiable information contained within messages by securing them with best practice encryption at rest and in transit, whilst also requiring two-factor authentication to access messages.

Zivver also provides out-of-the-box business rules that can be used to alert users with real-time visual warnings that personal identifiable information must be sent securely and/or if they are about to send PII to the incorrect recipient, thus preventing noncompliance with data protection legislation.

zivver

Zivver
5 New Street Square
EC4A 3TW London
United Kingdom

+44 (0) 203 285 6300
contact@zivver.com

www.zivver.com

linkedin.com/company/zivver
facebook.com/zivver
@zivver_en