



[WHITEPAPER]

HOW TO ACHIEVE REGULATORY COMPLIANCE WITH INSTASAFE (ISO 27001, HIPAA, GDPR, PCI DSS)

JAN 2024

INTRODUCTION

InstaSafe empowers organizations in their cybersecurity transformation journey, by enabling employees to safely and securely access enterprise applications (private and public) from anywhere on any network, with enhanced security, seamless experience, and minimal risk.

This document details how InstaSafe can help organizations meet various compliance regulations and security requirements.

- ISO/IEC 27001: 2022: Information Security Management System
- HIPAA: Health Insurance Portability and Accountability Act
- GDPR : General Data Protection Regulation
- PCI DSS: Payment Card Industry Data Security Standard

ISO/IEC 27001: 202

Recommended Security Controls	How can InstaSafe help?
A.9 Access Control	
Access of networks and network services	InstaSafe Zero Trust Access provides least privilege access to users ensuring only the right users get access to the network / network resources after proper authentication & authorization mechanisms
User Access Provisioning	InstaSafe controller manages users and user groups based on roles. User provisioning is managed by IT admin based on user's role and user's need.
Management of privileged access right	Privileged user management controls are in place within InstaSafe which helps to provide an effective access control mechanism for privileged users.
Removal or adjustment of access rights	In case of termination of any employee or third party contractor, users can be removed from the InstaSafe controller, thereby all access is revoked at once.
Information Access Restriction	InstaSafe limits access to enterprise applications to users based on least privilege access. Access is provided on a "Need to know basis" based on user roles.
Secure Logon Procedures	InstaSafe Multi-factor Authenticator provides a secure authentication mechanism covering Biometric authentication, push authentication, T-OTP, Hardware and certificate based authentication.
Password Management System	InstaSafe enforces strong password policy which involves combination of alphanumeric characters and special character and password expiry.
Access Control to Program Source Code	InstaSafe provides secure gateway where enterprises can manage their program source code behind InstaSafe gateway with added dropall firewall

Recommended Security Controls	How can InstaSafe help?
A.12.4 Logging and Monitoring	
Event Logging	InstaSafe Zero Trust provided detailed logs of entire user and network activity pertaining to user login details, application access details, and network gateway health status

Recommended Security Controls	How can InstaSafe help?
A.13.1 Network Security Management	
Network Controls	InstaSafe Zero Trust Gateway protects the enterprise network with drop-all firewall and limit access to users which is authenticated by the controller.
Segregation in networks	InstaSafe creates network segmentation based on Application and application group and restricted access is provided based on 'Need to Know' basis

GDPR (GENERAL DATA PROTECTION REGULATION)

GDPR Requirement	How can InstaSafe help?
Follow “Data Protection by Design and by Default”	InstaSafe takes adequate security controls in storing and managing customer data. From user device to application server, the data flows in an encrypted tunnel (mTLS and AES256 encryption)
Use encryption or pseudonymization whenever feasible.	All data traffic that flows from user device (with InstaSafe ZT agent installed) to application server (protected by InstaSafe Gateway) is fully end-to-end encrypted.
Right to see and request what personal data you have about them	InstaSafe deal with enterprise customers and obtain their approval to store and manage their data, further helping them in managing secure access to their enterprise resources. InstaSafe can provide information of data stored on request in compliance with GDPR.
Request to ask for data deletion	Upon an enterprise customer’s request, InstaSafe deletes requested data from its servers and backup copies if any.
Provide clear information about data processing	InstaSafe mention in its privacy policy on the type of user information it captures to provide secure access for their enterprise resources. InstaSafe works closely with Enterprise security team in defining the scope of data to be captured.

HIPAA: HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT

HIPAA Requirement	How can InstaSafe help?
Administrative Safeguards	
<i>Security Management Processes:</i> implement security measures that reduce risks and vulnerabilities to a reasonable and appropriate level.	InstaSafe Zero Trust Access provides Multi-factor authentication, least privilege access and end to end encrypted data traffic to help organization reduce cybersecurity risks arising out from insecure application access.
<i>Information Access Management:</i> to implement policies and procedures for authorizing access with appropriate role-based access consistent with the Privacy Rule “minimum necessary” standard	InstaSafe Zero Trust Access provides Role Based Access Control (RBAC) for users and user groups with least privilege access to ensure right users get access to only authorized applications after strict authentication controls
Physical Safeguards	
<i>Workstation and Device Security:</i> implement policies and procedures to specify the proper use of and access to workstations and electronic media.	InstaSafe ensures only the trusted and compliant devices are given access to enterprise critical resources after proper authentication mechanisms. InstaSafe agent analyses more than 15 device parameters to check the device compliance status and only then allows access
Technical Safeguards	
<i>Access Controls:</i> implement technical policies and procedures that allow only authorized persons	InstaSafe provides Role Based Access Controls (RBAC) to access enterprise resources. After proper authentication controls using MFA, authorization is provided to the right user.
<i>Person or Entity Authentication:</i> Implement procedures to verify that a person or entity seeking access to electronic information is the one claimed	InstaSafe enforces Multi-factor authentication which combines 3 parameters ‘Something you are’, ‘Something you have’ and ‘Something you know’. It supports OTP, T-OTP, Push notification, Biometrics (Facial and Fingerprint), Hardware token (Yubikey) and certificate based authentication

PCI DSS: PAYMENT CARD INDUSTRY DATA SECURITY STANDARD

PCI DSS Requirement	How can InstaSafe help?
Build and Maintain a Secure Network	InstaSafe provides secure gateway with built in dropall Firewall controls ensuring secure network environment. InstaSafe Zero Trust Access also provides Role Based Access Control (RBAC) for users with least privilege access to ensure right users get access to networks after strict authentication controls.
Do not use vendor-supplied defaults for system passwords and other security parameters	InstaSafe don't provide any default user and password for any of its customer. InstaSafe can enforce organization defined password policy for its users. Using Device Posture check control, InstaSafe can ensure only compliant devices get access to enterprise resources.
Use and regularly update anti-virus software or programs	InstaSafe can push patch updates and group policies to on-site and remote employees so that users always stay secure and compliant. Using Device Posture check control, InstaSafe can ensure only compliant devices get access to enterprise resources.
Assign a unique ID to each person with computer access	InstaSafe enforces multi-factor authentication along with device security posture check which ensures right user with right device is accessing the enterprise resources
Maintain a policy that addresses information security for employees and contractors	For contractors, contextual application access is provided based with added controls such as time based access, Geolocation based access, IP based access. For employees, only trusted and compliant devices are given access. Enterprise can create rule based access for contractors and internal employees separately.

REFERENCE DOCUMENTS:

1. ISO/ IEC 27001: 2022 - https://www.cssia.org/wp-content/uploads/2020/01/ISO_27001_Standard.pdf
2. GDPR: <https://gdpr.eu/checklist/?cn-reloaded=1>
3. HIPAA:
<https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/security101.pdf>
4. PCI DSS: https://www.commerce.uwo.ca/pdf/PCI-DSS-v4_0.pdf

ABOUT INSTASAFE

InstaSafe's mission is to secure enterprises from the abuse of excessive trust and privilege access. We empower organizations across the globe in preparing their security infrastructure for digital transformation in a cloud-dominated world. Recognized by Gartner as one of the top representative vendors providing Zero Trust Security, InstaSafe Secure Access, InstaSafe Zero Trust Application Access, and InstaSafe Authenticator follow the vision that trust can never be an entitlement, to offer securely enhanced and rapid access of enterprise applications to users situated anywhere across the globe. We secure 500,000 endpoints for more than 150 customers, spread across 5 continents, with our 100% cloud-delivered solutions, ensuring that our offerings are in line with our mission of being Cloud, Secure, and Instant.


PROBLEMS? TALK TO US


Let's talk more about how InstaSafe can empower your remote workforce through transformational and seamless security.


✉ sales@instasafe.com


🌐 www.instasafe.com

You can connect us at:

 /instasafe

 /instasafe

 /instasafe

 /instasafeZT