HOMOLOGATION WITH THE GENERAL INFORMATION SECURITY TERMS OF RIMAC SEGUROS Y REASEGUROS

By signing this document, the SUPPLIER, represented by its signing attorneys-in-fact, who declare that they have sufficient authority to consent to this type of document, undertakes to strictly comply with each of the obligations set forth below regarding the Information Security standards and conditions applicable to the processing of RIMAC SEGUROS information:

1. Safeguards

Whenever the SUPPLIER stores, processes, or transfers RIMAC SEGUROS information, it shall maintain administrative, technical, and physical controls intended to ensure the privacy, integrity, and confidentiality of RIMAC Information (the “Safeguards”) in accordance with applicable good practices, standards, and laws, including the following:

1.1 Physical access

The SUPPLIER shall maintain physical access controls designed to secure the relevant facilities, infrastructure, data centers, hard-copy files, servers, backup systems, and equipment, including mobile devices, used to Access RIMAC Information in connection with the contracted service, including controls to prevent, detect, and respond to attacks, intrusions, or other system failures.

1.2 User authentication

The SUPPLIER shall maintain user authentication, including the use of two-factor authentication and other secure standards currently prevailing in the market, as well as access controls and the assignment of specific privileges within operating systems, applications, equipment, and media.

1.3 Personal Security

The SUPPLIER shall maintain personnel policies and practices that restrict Access to RIMAC Information, including written confidentiality agreements, and shall conduct background checks in accordance with Applicable Laws for all personnel who Access RIMAC Information or who maintain, implement, or administer its information security program and the Safeguards.

1.4 Logging and Monitoring

The SUPPLIER shall log and monitor the details of all Access to Protected Information on the networks, systems, and devices operated by the SUPPLIER. Its logging and monitoring systems must comply with the Applicable Standards, and the SUPPLIER shall retain all Access logs for at least 90 days.

1.5 Malicious Software Controls

The SUPPLIER shall maintain current, market-leading controls to protect all networks, systems, and devices that Access RIMAC Protected Information against malware and unauthorized software.

1.6 Security Patches

The SUPPLIER shall maintain controls and processes designed to ensure that its technology infrastructure, systems, and devices, including operating systems and applications, that access, store, and/or process RIMAC Information are kept up to date. This includes the immediate implementation of all security patches when issued and/or when required to remediate security vulnerabilities.

1.7 User Account Management

The SUPPLIER shall implement management procedures to securely create, modify, and delete user accounts on the networks, systems, and devices through which the SUPPLIER Accesses RIMAC Information. This includes controlling privileged accounts and ensuring that RIMAC information owners duly authorize all user account requests.

The SUPPLIER is responsible for protecting and safeguarding the access credentials, including usernames and passwords, identification badges, and physical access cards, assigned by RIMAC exclusively for the SUPPLIER's use in performing its duties, taking into account that such credentials provide access to RIMAC's various information systems and physical premises.

The SUPPLIER understands and accepts that access credentials are for personal use and must not, under any circumstances, be disclosed, transferred, or shared with third parties. The SUPPLIER acknowledges that it is responsible for every action performed using the access credentials assigned in RIMAC's information systems and for any consequences arising from possible misuse. If credentials assigned to the SUPPLIER are compromised, the SUPPLIER shall immediately notify RIMAC.

2. Confidentiality

The SUPPLIER must protect all confidential information accessed in connection with the services it provides, ensuring that such information is not disclosed to third parties without RIMAC's prior consent, except where required by law.

3. Personal Data Protection

The SUPPLIER undertakes to comply with applicable data protection regulations and to implement the security measures necessary to ensure the privacy of the personal data processed, preventing unauthorized access, alteration, loss, or improper processing.

4. Access Controls

Whenever the SUPPLIER stores, processes, or transfers RIMAC information, it shall maintain security controls so that only authorized personnel have access to sensitive data through secure authentication

methods. The SUPPLIER must also ensure that access is granted only to personnel with a legitimate need to access the information under the Contract. The SUPPLIER is responsible for immediately notifying RIMAC when any employee assigned to provide the service ceases employment with the company, so that the applicable system deprovisioning processes can be carried out and RIMAC information safeguarded.

5. Encryption Requirements

Whenever the SUPPLIER stores, processes, or transfers RIMAC information, it shall use a current encryption standard that has not been compromised in the global market.

The SUPPLIER shall consider encrypting information in each state:

- Data at rest: encryption shall be considered for information storage.
- Data in transit: transmission encryption shall be considered, including certificates, private networks (VPNs) and/or secure communication protocols, firewalls, and intrusion detection systems.
- Data in use: in-memory encryption shall be considered, including volatile memory or secure servers.

6. Training and Oversight

As part of its activities, the SUPPLIER shall provide ongoing training and oversight, at least annually, on information security, privacy, and information protection to all personnel involved in providing the service whenever they access RIMAC information or resources, including third-party suppliers. Training must include good practices, sensitive data handling, security procedures, and incident response.

With regard to awareness, the SUPPLIER must conduct programs to foster an information security culture, including phishing tests, secure password management, and prevention of cyberattacks. The SUPPLIER shall conduct Information Security competency assessments to verify that employees supporting the service correctly apply the security practices taught. These assessments must be monitored, and reinforcement plans must be established for those who do not achieve the required level.

RIMAC may require the SUPPLIER to provide any additional training that RIMAC reasonably considers necessary for the SUPPLIER to comply with the contracted service, as well as evidence of the training and awareness campaigns conducted.

7. Use of RIMAC Seguros networks, systems or devices

To the extent that the SUPPLIER accesses networks, systems, or devices owned or managed by RIMAC, including Application Programming Interfaces (APIs), corporate email accounts, equipment, or RIMAC SEGUROS facilities, in order to access Information, it shall comply with the instructions set out below:

The SUPPLIER undertakes to ensure that all personnel responsible for providing services to RIMAC SEGUROS use electronic equipment or devices, such as computers, laptops, tablets, or other devices, provided by the SUPPLIER. Accordingly, the SUPPLIER undertakes to ensure that its personnel do not, under any circumstances, use personal laptops or equipment and/or equipment not provided by the SUPPLIER to perform their duties, including the provision of services to RIMAC SEGUROS.

The SUPPLIER undertakes to ensure that such equipment complies with the security and quality specifications established by RIMAC SEGUROS, as set out in Annex I to this document.

The SUPPLIER undertakes to keep permanently available to RIMAC SEGUROS all evidence supporting that the electronic devices meet the security specifications required by RIMAC SEGUROS under Annex I. At RIMAC SEGUROS' sole request, the SUPPLIER shall submit such evidence within a maximum of three (3) business days from the date on which the information is requested.

The SUPPLIER acknowledges and accepts that RIMAC SEGUROS reserves the right to conduct audits at any time during the term of the services to verify compliance with these guidelines. RIMAC SEGUROS shall notify the SUPPLIER of the date and time of the audit.

Notwithstanding any confidentiality obligations established in the employment agreements entered into by the SUPPLIER with its employees, the SUPPLIER's employees assigned to perform the service provided to RIMAC SEGUROS shall declare their adherence to the Supplier Code of Conduct and undertake to comply with the information security policies established by RIMAC SEGUROS.

8. Assessments, Audits and Remediation

8.1 Rimac Security Assessment

If requested by RIMAC, the SUPPLIER shall permit, on a coordinated and mutually agreed basis, any assessment intended to verify information security controls, whether performed by RIMAC and/or by a third party authorized for such purpose. RIMAC shall send the request at least fifteen (15) calendar days before the audit, and the SUPPLIER shall respond no later than fifteen (15) calendar days after the assessment requirements are sent. RIMAC shall treat the information provided by the SUPPLIER during the assessments as the SUPPLIER's confidential information.

In addition, RIMAC may conduct on-site visits, subject to prior coordination with the SUPPLIER, to gather evidence regarding technical or management controls implemented to ensure the security of RIMAC information.

8.2 Vulnerability Testing

If the SUPPLIER stores, processes, or transfers information, or accesses RIMAC technology resources from its systems, or if its systems connect to RIMAC's network or internal systems, RIMAC may request from the SUPPLIER a technical vulnerability testing report, including supporting evidence that the SUPPLIER's resources have no vulnerabilities or only low-impact vulnerabilities. Otherwise, RIMAC may require the SUPPLIER to provide the mitigation or remediation actions taken in relation to vulnerabilities detected in the technology resources used to provide services to RIMAC.

8.3 Supplier Self-Assessment

The SUPPLIER shall conduct continuous monitoring to properly manage risks to RIMAC Information and ensure that the Safeguards are properly designed and maintained to prevent unauthorized Access to RIMAC Information. Periodically, and at least once a year, the SUPPLIER shall assess and document the effectiveness of its Safeguards across the networks, systems, and devices, including infrastructure, applications, and services, used to access RIMAC Information. The SUPPLIER shall provide RIMAC with the results of the vulnerability test performed and the status of any corrective measures arising from its conclusions. RIMAC shall treat these results as the SUPPLIER's confidential information.

8.4 Audits, Certifications and Reports

The SUPPLIER shall permit privacy and information security audits to be conducted on a coordinated and mutually agreed basis with RIMAC by designated RIMAC personnel, an external audit firm, or a domestic or foreign firm able to demonstrate the required knowledge and experience.

In lieu of an audit initiated by RIMAC, and at RIMAC SEGUROS' option, the SUPPLIER shall make available to RIMAC its most recent penetration testing report, latest audit report, or certification evidencing its compliance with this Contract, including its most recent ISO 27001 certification, SOC 1 or SOC 2 reports, or Payment Card Industry (PCI) Attestation of Compliance relating to the Services. RIMAC shall treat these results as the SUPPLIER's confidential information.

If the SUPPLIER fails to facilitate the foregoing, a report shall be issued documenting non-compliance with information security controls, and the relevant RIMAC business area shall be informed of the identified risks affecting the confidentiality, integrity, and availability of information within the scope of the service, so that the appropriate actions may be taken with the SUPPLIER.

8.5 Remediation of Vulnerabilities and Audit Findings

If either party identifies a vulnerability in the SUPPLIER's Safeguards or findings resulting from audits conducted by RIMAC or an external audit firm authorized by RIMAC, the SUPPLIER shall immediately remediate or mitigate, at its own cost, each vulnerability or finding within a period determined by its criticality, and in no event later than thirty (30) days for vulnerabilities and findings classified as critical, sixty (60) days for those classified as high, and ninety (90) days for those classified as medium. The SUPPLIER shall provide RIMAC SEGUROS with the corresponding closure evidence.

If RIMAC identifies vulnerabilities, the SUPPLIER shall provide reasonable assurance that its remediation meets the requirements of this Contract. If the SUPPLIER cannot remediate or mitigate the vulnerabilities within the specified period, it shall immediately notify RIMAC and propose reasonable measures. Compliance with this Section shall not reduce or suspend the SUPPLIER's obligations under Section 9, Security Incident Response, nor reduce or suspend RIMAC's rights under Sections 16.2, Suspension, and 16.3, Records and Retention.

9. Security Incident Response

9.1 Security Incident Response Program

The SUPPLIER shall maintain a reasonable Security Incident Response Program based on current market best practices. Any incident affecting the confidentiality, integrity, or availability of RIMAC information must be reported immediately, including the information described in Section 9.2.

9.2 Security Incident Notification

Upon becoming aware of any Security Incident, the SUPPLIER shall immediately take measures to minimize harm; secure RIMAC SEGUROS Information; notify RIMAC, in no event later than 24 hours after discovering the Security Incident, by emailing ciberseguridad@rimac.com.pe with the information described in the following paragraph; and communicate to RIMAC the measures and procedures carried out under Applicable Laws to mitigate the effects of the incident.

If requested, the SUPPLIER shall provide reasonable information regarding the Security Incident, including: a description of the Protected Information affected by the Security Incident, including the categories and quantity of data records and Data Subjects involved; the date and time of the Security Incident; a description of the likely consequences; a description of the circumstances that gave rise to the Security Incident, for example unauthorized access, including leakage, alteration, destruction or deletion, information theft, and service interruption; a description of recommended measures to mitigate any adverse effect; a description of the measures proposed by the SUPPLIER to address the Security Incident; and relevant contact persons who shall remain reasonably available until the parties mutually agree that the Security Incident has been resolved. For Security Incidents involving RIMAC Information, “reasonably available” means 24 hours a day, 7 days a week.

9.3 Corrective Measures

The SUPPLIER shall take appropriate measures to immediately correct the root cause or causes of any Security Incident and shall reasonably cooperate with RIMAC in the investigation and corrective measures relating to the incident. The SUPPLIER shall also immediately provide RIMAC with the investigation results and any corrective measures implemented.

9.4 Unathorized Statements

Unless otherwise required by Applicable Laws, the SUPPLIER shall not make, or permit any third party to make, any statement relating to a Security Incident that directly or indirectly refers to RIMAC SEGUROS without RIMAC’s express prior written authorization.

10. Acceptable Use of Information, Equipment and IT Services

10.1 Whenever the SUPPLIER stores, processes, or transfers information, or accesses RIMAC technology resources, it shall use them responsibly and solely in connection with the contracted service activities. The SUPPLIER shall also notify RIMAC of any event that may compromise IT resources or the information they contain.

10.2 If information must be exchanged as part of the service, the SUPPLIER and RIMAC shall coordinate delivery or exchange through secure communication channels mutually determined to meet the confidentiality, availability, and integrity requirements of both parties. The transmission of information through free or public services is prohibited.

11. Security for Acquisition, Development and Maintenance

11.1 The SUPPLIER shall align with and ensure that systems developed for RIMAC, or used to provide services to RIMAC, comply with secure development standards consistent with RIMAC’s standards for the configuration, development, and maintenance of required systems and applications, as set out in Annex II.

11.2 As part of the development lifecycle, the SUPPLIER must perform an application security assessment, including vulnerability analysis or Ethical Hacking, at the code and application levels before publication, in order to identify vulnerabilities and ensure that they are

remediated within the periods specified in Section 8.5, Remediation of Vulnerabilities and Audit Findings.

11.3 The SUPPLIER must ensure that periodic information is provided regarding updates or fixes made to the system or application and must provide the corresponding advice and support.

11.4 In coordination with RIMAC, the SUPPLIER must make secure channels available for the exchange of information in a manner that ensures its integrity and confidentiality.

12. Compliance

12.1 The SUPPLIER must comply with the requirements established by RIMAC, as well as the controls required under the laws and regulations applicable to RIMAC, including Law No. 29733, the Personal Data Protection Law and its Regulations; SBS Circular G-140; and SBS Resolution No. 504-202, approving the Regulations for Information Security and Cybersecurity Management.

13. Secure Deletion of Information

13.1 Upon termination of employment of the SUPPLIER's personnel or upon completion of the service provided to RIMAC, the SUPPLIER shall securely delete all RIMAC information stored, processed, or generated on the equipment used to provide the service, in accordance with secure data disposal best practices. The SUPPLIER shall also formally confirm to RIMAC that the information has been deleted.

13.2 Upon termination of the contractual relationship or at RIMAC's request, the SUPPLIER shall cease using the confidential information, return to RIMAC all confidential information received, and destroy every copy made. In addition, the SUPPLIER shall provide written confirmation no later than 15 days after termination of the Contract.

14. Subcontracting by the Supplier

Whenever the SUPPLIER subcontracts personnel or any part of the contracted service, it must ensure that the subcontracted SUBCONTRACTOR complies with the requirements set out in this document. The subcontracted SUBCONTRACTOR must also have confidentiality and personal data protection agreements covering RIMAC information.

14.1 The SUPPLIER is responsible for notifying RIMAC within no more than fifteen (15) days of any change involving a subcontracted SUBCONTRACTOR engaged in the delivery of the service acquired by RIMAC.

14.2 If the SUPPLIER needs to subcontract any part of the service, it shall obtain RIMAC's authorization.

14.3 If the SUPPLIER needs to subcontract any part of the service, the new party shall comply with RIMAC's security guidelines.

15. Legal Process

If the SUPPLIER, or any person to whom the SUPPLIER provides Access to Protected Information, is legally compelled by a court or other governmental entity to disclose Protected Information, then, to the extent permitted by law, the SUPPLIER shall immediately notify RIMAC of the request and reasonably cooperate with RIMAC's efforts to challenge the disclosure, seek an appropriate protective order, or pursue any other legal action RIMAC considers appropriate. Unless required by Applicable Laws, the SUPPLIER shall not respond to such request unless authorized by RIMAC.

16. SPECIAL CATEGORIES OF DATA

16.1 Payment Card Industry Compliance

To the extent that the SUPPLIER stores, processes, or transmits cardholder information or other payment information on behalf of the entity, subject to the Payment Card Industry Data Security Standard (PCI DSS) in connection with its Services, it shall be responsible for the security of such information. The SUPPLIER shall ensure that it is currently and demonstrably certified or compliant with the PCI DSS standard, as documented by a qualified independent QSA auditor through a Report on Compliance (ROC) and Attestation of Compliance (AOC), and shall maintain its compliant status for as long as it Accesses such data in connection with the Contract.

16.2 Suspension

RIMAC may immediately suspend the SUPPLIER's Access to Protected Information if RIMAC reasonably determines that the SUPPLIER is not complying with this Contract or Applicable Law.

16.3 Records and Detention

16.3.1 Records

The SUPPLIER shall maintain at its ordinary place of business detailed, accurate, and current records relating to its Access to RIMAC Information, sufficient to demonstrate compliance with its obligations under this Contract. Upon request, the SUPPLIER shall make those records available to RIMAC SEGUROS. If the SUPPLIER Accesses RIMAC SEGUROS Information, such records shall contain at least:

- (a) its name and contact details;
- (b) the categories of recipients to whom RIMAC SEGUROS Information has been or will be disclosed;
- (c) the name and contact details of its data protection officer, if any;
- (d) the categories of processing activities performed on behalf of RIMAC SEGUROS; and
- (e) where applicable, information concerning international data transfers, including identification of the countries to which RIMAC Information is transferred and, where appropriate, documentation of suitable safeguards covering transfers of RIMAC SEGUROS Information.

16.3.2 Retention

The SUPPLIER shall not retain any RIMAC Information except to the extent necessary to provide the Services under the Contract. At RIMAC's request, the SUPPLIER shall immediately return a copy of RIMAC SEGUROS Information to RIMAC.

16.3.3 Media Sanitization

The SUPPLIER shall use a media sanitization process that deletes and destroys data in accordance with guidelines based on current market standards.

17. LIABILITY FOR SECURITY BREACHES

If a Security Breach in the systems used by the SUPPLIER to provide the service affects customer data, the SUPPLIER shall be responsible for covering mitigation costs and any associated liability arising therefrom, to the extent permitted by law.

18. Updating Security Measures

The SUPPLIER must update and improve its security measures as technologies evolve and new threats emerge, ensuring the ongoing protection of customer information.

19. Penalties

The SUPPLIER acknowledges and accepts that failure to comply with any obligation under these Terms shall result in a penalty imposed by RIMAC SEGUROS equivalent to 5% of the monthly invoice. RIMAC SEGUROS may offset such amount against the compensation or any other outstanding amount payable to the SUPPLIER. In the event of recurrence within a period of 12 months from the first penalty imposed, a penalty equivalent to 10% of the monthly invoice shall apply.

Without prejudice to the imposition of the penalty, non-compliance with the stated obligations may constitute grounds for automatic termination, for which purpose it shall be sufficient for RIMAC SEGUROS to send a notice to that effect to the SUPPLIER.

Date: _____

Legal or Corporate Name:

Taxpayer Identification Number (RUC):

Name of Legal Representative 1: _____

National Identity Document (DNI) of Legal Representative 1:

_____

Signature: _____

Name of Legal Representative 2: _____

National Identity Document (DNI) of Legal Representative 2:

_____

Signature: _____

ANNEX I

REQUIREMENT	MINIMUM SPECIFICATION	COMMENTS	CONDITION
Operating System	Windows 11 - x64 - 24H2; macOS 15 (Sequoia) or later; macOS 14 (Sonoma) until Aug. 2026	Security recommends these minimum versions so hosts receive current patches. The user must not be a local administrator of the laptop.	Required
Security Patches	Up-to-date patching	Automatic operating-system updates are recommended unless the supplier's current management process permits timely OS patching. A process for patching or updating software installed on the operating system is also recommended.	Required
Antimalware	Current standard version defined by the supplier	Up-to-date signature database.	Required
Endpoint DLP	Current standard version defined by the supplier	At minimum, content-control policies shall cover PCI DSS, Personal Data Protection Law (PII), insurance policies, HIPAA, and GDPR.	Required
Device Control	Current standard version defined by the supplier	Prevent files from being copied to storage devices, particularly USB, and prevent wireless file transfers such as Bluetooth.	Required
EDR Endpoint Agent	Current standard version defined by the supplier	Up-to-date agent and indicators of compromise.	Required
Application Control	Current standard version defined by the supplier	The supplier shall control the software approved for use by its personnel.	Desired
Cloud Productivity Suite	Microsoft 365	If RIMAC provides collaboration tools, the supplier shall have at least Microsoft 365 F1 or F3 and Microsoft Defender for Office 365 Plan 1 licenses in the rimac.com.pe tenant, enabling Intune, MFA, auditing, anti-phishing, Safe Attachments, Safe Links, anti-spam, antimalware, Cloud DLP, and internal-only collaboration. If licenses are supplier-provided and tenant-managed, controls shall be aligned and reinforced with CASB.	Required
Threat Management Agent	Current standard version defined by the supplier	If not part of the supplier baseline, RIMAC's Red Team may define a scanning	Desired

		process to identify configuration deviations.	
Endpoint Encryption	Current standard version defined by the supplier		Required
VPN Client	FortiClient VPN - latest version published by Fortinet		Required
NAC Agent	Aruba - latest stable standard version defined and certified by RIMAC	RIMAC-managed service; only the agent would be installed to provide visibility into software and local access to the RIMAC network.	Required
Browser	Microsoft Edge and Google Chrome, up to date	Apply supplier-defined policies for hardening and secure browsing. Mozilla Firefox must not be installed.	Required
URL Filtering	Not applicable	A browsing profile shall block public streaming, cloud storage, personal email, social media, file-transfer services, and other categories prone to data leakage, leisure use, or poor reputation. Access shall be limited to RIMAC-related sites and services, with DLP controls for uploads to personal or unrelated services.	Required
Security Configuration	Security baseline defined by the supplier	Hardening shall cover local-user administration, local auditing, secure user-rights and security options, and disabling insecure or unnecessary Windows services such as SMBv1, TFTP, and Telnet Client.	Required
Other - VDI	Clipboard	For remote work through a virtual desktop over HTTPS or VPN, disable clipboard functionality to prevent copying files from the RIMAC virtual desktop to the host PC.	Required
Other - VDI	Restrict Command Prompt access	Use of cmd.exe and PowerShell shall be restricted.	Required
Other - VDI	Not applicable	Whether on-premises or cloud-based, authorization shall permit access only from RIMAC's internal network, not from the Internet.	Required
Other - VDI	Restrict local administrator access	The supplier user must not be a PC administrator.	Required

ANNEX II

The following sections are established as security controls in the development lifecycle:

1. Error Handling and Logging

BEST PRACTICE	DESCRIPTION
1.1 Display generic error messages	Error messages must not reveal details about the application's internal state, including platform versions and names, file-system paths, or stack information.
1.2 Do not disclose excessive information in error messages	Authentication error messages must be clear without disclosing confidential system information. For example, stating that a user ID is valid but its password is incorrect confirms that the account exists.
1.3 No unhandled exceptions	For the languages and frameworks used in web application development, unhandled exceptions must never be permitted. Error handlers shall manage unexpected errors and return controlled results.
1.4 Suppress framework-generated errors	Default messages generated by frameworks or platforms shall be suppressed or replaced with custom error messages because they may reveal confidential information.
1.5 Log all authentication activity	All authentication activity, whether successful or unsuccessful, must be logged.
1.6 Log all privilege changes	Every activity or event in which a user's privilege level changes must be logged.
1.7 Log administrative activities	All administrative activity in the application or any component must be logged, as must business-defined critical activities.
1.8 Log access to confidential data	Every access to confidential data must be logged, particularly where regulatory or contractual requirements apply, including the Personal Data Protection Law and PCI.
1.9 Do not log inappropriate data	Confidential data must never be logged in unencrypted form. Under PCI, logging confidential data without encrypted logs may constitute a violation and create a serious exposure point.
1.10 Store logs securely	Logs shall be stored and maintained to prevent loss or tampering. Retention shall align with audit logging and Operations Security policies and support forensic and incident-response activities.

2. Data Protection

BEST PRACTICE	DESCRIPTION
2.1 Use HTTPS everywhere	HTTPS should ideally be used throughout the application and must, at minimum, protect authentication pages, all post-authentication pages, and any pre-authentication feature through which confidential information can be sent.
2.2 Disable HTTP access for all protected resources	Any URL requiring HTTPS protection must not be accessible through an insecure HTTP channel.
2.3 Use the Strict-Transport-Security header	The Strict-Transport-Security header ensures that the browser does not communicate with the server over HTTP.
2.4 Store user passwords using strong, iterative salted hashing	Use secure hashing techniques and strong algorithms such as PBKDF2, bcrypt, or SHA-512, with adaptive hashing and a salt.
2.5 Exchange encryption keys securely	Any exchange or establishment of encryption keys must take place through a secure channel.
2.6 Configure secure key-management processes	Stored keys must be properly secured and accessible only to appropriate personnel as needed, for example through AWS KMS, Azure Key Vault, or AWS CloudHSM.
2.7 Weak TLS configuration on servers	Disable weak ciphers on all servers and use at least TLS 1.2. Disable SSL v2, SSL v3, pre-1.2 TLS, NULL, RC4, DES, and MD5 cipher suites; use key lengths over 128 bits, secure renegotiation, and no compression.
2.8 Use valid HTTPS certificates from a reputable CA	HTTPS certificates must be signed by an accredited certification authority, match the website FQDN, and be valid and unexpired.
2.9 Disable data caching through cache-control and autocomplete settings	Disable browser caching through HTTP headers or HTML meta tags. Sensitive input fields such as login forms shall use autocomplete=Off.

2.10 Limit the use and storage of confidential data	Assess whether confidential data is transported or stored unnecessarily and use tokenization where possible.
2.11 Need to use confidential data	Functional analysts shall assess with business areas whether data classified as Confidential Information needs to be extracted and displayed.
2.12 Display of confidential data	Functional analysts and developers shall assess which roles or profiles need to view confidential personal, health, banking, or similar data and apply non-display or masking where full access is unnecessary.
2.13 Protection of banking data	New developments or system changes capturing customer banking data shall use front-end obfuscation or masking and protect database records in line with applicable PCI DSS requirements, including card-number encryption where storage is strictly necessary.

3. Configuration and Operations

BEST PRACTICE	DESCRIPTION
3.1 Automate application deployment	Continuous integration and deployment help ensure consistent and repeatable changes across environments.
3.2 Establish a rigorous change-management process	A rigorous change-management process shall be maintained, and new versions shall be deployed only after the required process.
3.3 Define security requirements	Engage the business owner to define security requirements, including allowlist validation rules and non-functional requirements, so security is integrated into the system from the outset.
3.4 Perform a design review	Conduct risk reviews and threat modelling to identify key risks and incorporate appropriate countermeasures into design and architecture.
3.5 Perform code reviews	Security-focused code reviews may be performed using automated tools or manually by personnel other than the original developer.
3.6 Perform security testing	Test during and after development and after major releases to verify compliance and ensure vulnerabilities are not introduced before production.
3.7 Harden infrastructure	Configure all supporting infrastructure components in accordance with security and hardening best practices, including routers, firewalls, switches, operating systems, web and application servers, databases, and frameworks.
3.8 Credentials in source code	Decouple environment-specific technical configurations from source code and manage them through secrets and configuration repositories such as Vault or AWS Parameter Store.
3.9 Code repositories	Use of RIMAC-managed GitLab and RIMAC's corporate GitHub repository is permitted. Publishing RIMAC source code in external public or unofficial repositories is prohibited.
3.10 Define an incident-handling plan	Incident handling shall be managed and governed under RIMAC's Security Incident Response process.
3.11 Do not hard-code credentials	Credentials must not be stored directly in application code or plain text; anonymization must be ensured.

4. Security Controls in Devsecops Pipelines

BEST PRACTICE	DESCRIPTION
4.1 Security controls in DevSecOps pipelines	Builds deployed to production must not generate security alerts; automated builds shall stop upon detection. In pre-production environments, monitoring mode may alert while allowing builds so responsible teams can remediate.
4.2 Automated web application and API review - dynamic analysis tool	The URLs scanned by RIMAC's acquired tool shall be reviewed periodically until licensed coverage is achieved.

4.3 Secret detection in the repository	Every new pipeline shall automatically detect secrets using the OpenSource Yield tool.
4.4 Use of OpenSource security controls in the pipeline	Open-source security tools may be incorporated where RIMAC has no licensed alternative or no available license coverage. Cases must be substantiated and communicated to the Security CoE through the Security Advisor on the DevSecOps team.

5. Authentication

BEST PRACTICE	DESCRIPTION
5.1 Develop a strong password-reset system	Password-reset systems shall use questions resistant to guessing and brute force and must not reveal whether an account is valid.
5.2 Implement a secure password policy	Applications shall reflect RIMAC's password policy, including session management and password reuse.
5.3 Implement account lockout against brute-force attacks	Implement lockout for authentication and password-reset functions. After repeated attempts, lock the account for a configurable period or until administrator unlock; keep generic error messages.
5.4 Store database credentials securely	Business-logic credentials used to connect to databases shall be stored in a locked, centralized location. Dispersing credentials throughout source code is unacceptable.
5.5 Key management	Maintaining sensitive information in source code, including database, application-user, or AWS Access Key and Secret Key credentials, is prohibited.
5.6 Applications and middleware should run with least privilege	Configure applications and middleware services to run with minimum privileges and do not provide administrative credentials granting access to unrelated databases or tables.

6. Session Management

BEST PRACTICE	DESCRIPTION
6.1 Ensure session identifiers are sufficiently random	Generate session tokens using secure random functions with sufficient length to resist analysis and prediction.
6.2 Regenerate session tokens	Regenerate tokens when a user authenticates, privilege level changes, or encryption status changes.
6.3 Implement an idle-session timeout	Automatically log out inactive users, considering recurring Ajax calls that may reset timeout counters.
6.4 Implement an absolute session timeout	Require logout after a long period, for example 4 to 8 hours, to mitigate hijacked-session risk.
6.5 Destroy sessions upon any sign of tampering	Detect session cloning where multiple sessions are not required and destroy suspicious sessions, requiring re-authentication.
6.6 Invalidate the session after logout	Destroy the session and related server-side data when the user logs out.
6.7 Place a logout button on every page	Provide an easily accessible logout button or link on each authenticated page.
6.8 Use secure cookie attributes	Set session cookies with HttpOnly and Secure flags.
6.9 Set cookie domain and path correctly	Use the most restrictive domain and path scope; wildcard-domain cookies require sound justification.
6.10 Set cookie expiration time	Use a reasonable expiration time and avoid non-expiring session cookies.

7. Mobile

BEST PRACTICE	DESCRIPTION

7.1 Verify identifier values	Do not use device identifiers retrievable by other applications, such as IMEI numbers, as authentication tokens.
7.2 Protect sensitive data	Sensitive data must not be stored unprotected on the device.
7.3 Delete sensitive information	Overwrite sensitive information in memory as soon as it is no longer required to mitigate memory-dump attacks.
7.4 Accessibility	Verify that passwords, secret keys, and API tokens are generated dynamically in the mobile application.

8. Input and Output Handling

BEST PRACTICE	DESCRIPTION
8.1 Perform contextual output encoding	Encode output contextually before sending it to the user, applying encoding appropriate to HTML, URL, JavaScript, or other contexts.
8.2 Prefer allowlists to blocklists	Validate every user input field. Prefer allowlists that accept only data meeting defined criteria; use blocklists where additional flexibility is needed.
8.3 Use parameterized SQL queries	Pass user content through bind variables. Do not dynamically construct SQL queries through string concatenation or user input.
8.4 Use tokens to prevent forged requests	Embed an unpredictable, request-specific CSRF token in HTML forms.
8.5 Configure encoding for the application	Define page encoding through HTTP headers or HTML meta tags and use a consistent encoding such as UTF-8.
8.6 Validate uploaded files	Validate file size, file type, content, and destination-path controls.
8.7 Use the nosniff header for uploaded content	Use X-Content-Type-Options: nosniff so browsers do not guess the data type of user-uploaded content.
8.8 Validate the input source	Reject input from an unexpected source, such as a GET variable where POST input is expected.
8.9 Use the X-Frame-Options header	Use X-Frame-Options to prevent foreign sites from framing content and mitigate clickjacking; use framebusting only for legacy browsers.
8.10 Use secure HTTP response headers	Content-Security-Policy and X-XSS-Protection headers help defend against Cross-Site Scripting.
8.11 Use Referrer-Policy response headers	Web application HTTP headers shall contain Referrer-Policy to help preserve HTTPS navigation.

9. Access Control

BEST PRACTICE	DESCRIPTION
9.1 Apply access-control checks consistently	Apply complete mediation by routing every request through a common security gatekeeper, regardless of authentication status.
9.2 Apply the principle of least privilege	Use mandatory access control and deny access unless explicitly allowed. Rights shall be specifically assigned to accounts, and the system shall support specific roles.
9.3 Do not use direct object references for access-control checks	Do not allow manipulable direct references to files or parameters. Base access decisions on authenticated identity and trusted server-side information.
9.4 Do not use unvalidated forwards or redirects	Unvalidated forwards may expose private content and redirects may lure users to malicious sites. Perform access-control checks before forwarding or redirecting.