Information Security

Version 2.0 – Dated May 15, 2024

1. Commitment to Information Security

With an understanding that ensuring information security is one of the most critical tasks of the management, Acsia will ensure that every person engaged in its operations will be committed to it.

2. Information Security Policy

Acsia is committed to ensuring Confidentiality, Integrity, and Availability of business information accessed, processed, stored, or exchanged as part of business operations in all stages of the information life cycle by implementing industry-standard policies and processes optimally defined to meet Organizational objectives, with a commitment for continual improvement involving all stakeholders of the Organization".

3. Protection of Information Assets

Acsia will institute appropriate management measures according to the state of individual operations to unfailingly protect information assets from any threat to its confidentiality, integrity, and availability.

4. Compliance with Laws and Regulations

Acsia will comply with applicable laws and regulations, other rules, and contractual requirements to ensure information security.

5. Education and Training

Acsia will offer education and training to personnel engaged in its operations to improve their awareness of information security and familiarize them with the Information Security Policy.

6. Prevention of Accidents and Actions

Acsia will run its information security management system to ensure that every employee works to prevent information security accidents from occurring. Should an accident take place, we will swiftly implement appropriate actions, including those for preventing recurrence.

7. Auditing

Acsia will regularly audit the operation of its information security management system and carry out remedial actions as needed to maintain information security.

8. Continuous Improvement

Every year we set information security goals, define, and plan activities to achieve those objectives, then, according to periodical review results, set the following year's goals. In addition, we regularly evaluate and review our Information Security Policy, its related internal regulations, and our management system, pursuing continuous improvement of information security.

9. Acsia Platform Security Commitments

- Protect the confidentiality and integrity of Acsia platforms and sensitive information
- Provide uptime and availability to the Platforms and associated services as stated in customer agreements
- Ensuring quality, accuracy, and security of the Platforms and data therein
- Ensuring security, confidentiality, and integrity of data coming in contact with third parties

10. Data Security Measures

Acsia has implemented and will maintain appropriate technical and organizational security measures to protect customer personal data from security incidents and to preserve the security and confidentiality of the customer personal data ("Security Measures"). The Security Measures applicable to the Services are as follows:

a) Web Application Penetration Test: Acsia shall continue to annually engage in web application penetration testing. Upon any customer's written request, we will provide the executive summary of the report to the Customer. We will address all medium, critical and severe vulnerabilities in the findings of the report within a reasonable, risk-based timeframe.

b) Security Awareness Training: Acsia will provide annual security training to all personnel. "Security Training" shall address security topics to educate users about the importance of information security and safeguards against data loss, misuse or breach through physical, logical and social engineering mechanisms. Training materials will address industry-standard topics which include, but are not limited to:

- The importance of information security and proper handling of PII
- Physical controls such as visitor protocols, safeguarding portable devices and proper data destruction
- Logical controls related to strong password selection/best practices
- How to recognize social engineering attacks such as phishing

c) Vulnerability Scan: Acsia shall ensure that vulnerability scans are performed on servers continuously and network security scans are completed at a minimum biannually, in each case using an industry-standard vulnerability scanning tool.

d) Employee-Related Policies:

- Unauthorized persons will be prevented from gaining physical access to our premises and the rooms where data processing systems are located.
- Employees will only be allowed access to tasks assigned to them.
- We will ensure that all computers processing personal data (including computers with remote access) are password protected, both after booting up and when left, even for a short period.
- We will assign individual user passwords for authentication. Passwords must include at least 8 characters, with both upper- and lower-case characters, at least one digit, and one symbol.
- We will only grant system access to our authorized personnel and strictly limit their access to applications required for those personnel to fulfill their specific responsibilities.
- We will implement a password policy that prohibits the sharing of passwords, outlines procedures to follow after disclosure of a password, and requires that passwords be changed regularly.
- We will ensure that passwords are always stored in encrypted form.
- We will have adopted procedures to deactivate user accounts when an employee, agent, or administrator leaves our employ or moves to another responsibility within the company.
- We will be able to retrospectively examine and establish whether and by whom your customer personal data has been entered into data processing systems, modified or removed.
- We will log administrator and user activities. Logs will include the Username, IP Address, Port Accessed, destination host access details. Acsia will retain the logs for 6 months.
- We will process the customer personal data received from different clients so that in each step of the processing the controller can be identified and so that data is always physically or logically separated.
- Employees are required to enable multi-factor authentication.

e) Process-Level Requirements: We will implement the following processes to ensure security and privacy:

- Acsia shall implement user termination controls that include access removal / disablement promptly upon termination of staff.
- Acsia shall have and maintain a patch management process to implement patches in a reasonable, risk-based timeframe.
- Acsia shall use firewall(s), Security Groups/VPCs, or similar technology to protect servers storing Customer Personal Data.
- Where Acsia handles customer personal data, servers shall be protected from unauthorized access with appropriate physical security mechanisms including, but not limited to, badge access control, secure perimeter, and enforced user provisioning controls (i.e. appropriate authorization of new accounts, timely account

- terminations and frequent user account reviews). These physical security mechanisms are provided by data center partners such as, but not limited to, AWS, Azure, and Google. All cloud-hosted systems shall be scanned, where applicable and where approved by the cloud service provider.
- Acsia will virtually segregate all Customer Personal Data in accordance with its established procedures. The Customer instance of Services may be on servers used by other non-Customer instances.
- Whenever an employee or contractor leaves or is terminated, that individual's access to customer user accounts shall be immediately terminated or disabled.

f) Application-Level Requirements:

- Acsia shall maintain documentation on overall application architecture, process flows, and security features for applications handling customer personal data.
- Acsia shall employ industry standard scanning tools and/or code review practices, as applicable, to identify application vulnerabilities.

g) Data-Level Requirements:

- Encryption and hashing protocols used for customer personal data in transit and at rest shall support NIST approved encryption standards (e.g. SSH, TLS).
- Acsia shall ensure that access to information and application system functions is restricted to authorized personnel only.
- Customer personal data stored on archive or backup systems shall be stored at the same level of security or better than the data stored on operating systems.

h) End User Computing Level Requirements:

- Acsia will require anti-virus scans with frequent signature updates for end-user computing devices to run at least weekly.
- Acsia will prohibit the use of removable media for storing or carrying customer personal data. Removable media include flash drives, CDs, and DVDs.

i) Compliance Requirements:

- Acsia will implement building access control to control and track access to its networks and other equipment.
- Acsia will determine each year which officers and employees within the company will have access to which categories of data and shall review this list annually at the executive level.

j) Personnel:

Acsia restricts its personnel from downloading and/or processing Customer Personal Data without authorization by Acsia as set forth in the Security Measures and shall ensure that any person who is authorized by Acsia to process Customer Personal Data is under an appropriate obligation of confidentiality.

k) Security Incident Response:

Upon becoming aware of a Security Incident, Acsia will notify the Customer without undue delay. Acsia will provide information relating to the Security Incident as it becomes known or

as is reasonably requested by the Customer to fulfill its obligations as a controller and will also take reasonable steps to contain, investigate, and mitigate any Security Incident.

l) ISO 27001:2022 Certification: Acsia has earned ISO27001 certification, and we go through an annual review.

m) TISAX Certification: Acsia has earned TISAX, a European automotive industry-standard information security assessment (ISA), and we go through a review every three years.

n) Data Minimization: Acsia will ensure that the personal data it collects and processes will be adequate, relevant, and limited to what is necessary to provide the Services

o) Data Retention and Destruction: Acsia will have in place secured destruction processes and will delete Customer personal data utilizing secure methods (equivalent to or greater than that of NIST SP-800-88 Rev. 1 or its successor guidelines) that render the data unreadable and unrecoverable.

p) Security Incident Response:

Upon becoming aware of any incident in which it suspects that unauthorized access has been gained to Acsia's systems, the executives of the company at the highest levels will be immediately notified.

- Executives will immediately confer with each other and with legal counsel regarding any security incident to ensure compliance with legal and contractual obligations.
- We will immediately investigate and mitigate any security incident.
- Acsia will obtain and maintain reasonable insurance to cover itself for cyber liability.

The response and resolution to a Security Incident & Weakness shall be as per the following scheme:

Priority Definition - Target Response - Target Resolution

- Major Incident - 10 Minutes - 4 Hours
- High - 30 Minutes - 8 Hours
- Medium - 1 Hour - 2 Days
- Low - 4 Hours - 5 Days
- Planning / Information Security Weakness - 2 Days - 10 Days