# ITARMI SECURITY STANDARDS

This document summarises the steps we take to ensure IT security for users of the Itarmi Platform.

## 1. GENERAL SECURITY MEASURES

We comply with industry standard security measures and all applicable data privacy and security laws and regulations, including with respect to personnel, facilities, hardware, software, storage, networks, access controls, vulnerability and breach detection, and incident response measures necessary to protect against unauthorised or accidental access, loss, alteration, disclosure or destruction of personal information provided to us. We apply security policies consistent with the International Organisation for Standardisation (ISO) 27001 standard.

## 2. INFORMATION SECURITY

We maintain the confidentiality, integrity and availability of our computer and data communication systems while meeting legal, industry and contractual requirements. We maintain an information security program that includes technical and organisational measures, as well as policies and procedures, to protect personal data processed by us against accidental loss; destruction or alteration; unauthorised disclosure or access; or unlawful destruction.

## 3. SECURE SOFTWARE DEVELOPMENT

We maintain policies and procedures to ensure that system, application and infrastructure development is performed in a secure manner. This includes reviewing and testing applications, products and services for common security vulnerabilities and defects, periodic penetration testing and security assessment of these services, defining baseline configurations and requirements for patching of third party systems.

## 4. HUMAN RESOURCES SECURITY

Our policy relating to personnel includes background checks, technical and other vetting procedures to ensure competence, acknowledgement of and adherence to our security policies, and termination for employees and third parties in appropriate circumstances.

## 5. DATA CLASSIFICATION & PROTECTION

We maintain policies and procedures for data classification and protection, together with requirements on data encryption, rules for transmission of data and requirements for removable media, along with requirements on how access to these data should be governed.

## 6. NETWORK SECURITY

We maintain policies and procedures in relation to the network infrastructure used to process Customer data, enforce safe network practices, and define service levels agreements with internal and external network services.

## 7. PHYSICAL & ENVIRONMENTAL SECURITY

We maintain policies and procedures for physical and environmental security, protecting areas that contain sensitive information and ensuring that critical information services are protected from interception, interference or damage.

## 8. BUSINESS CONTINUITY

We maintain a business continuity plan, as well as policies and procedures to ensure that we can continue to perform business critical functions in case of an extraordinary event. This includes data centre resiliency and disaster recovery procedures for business-critical functions.

## 9. ACCESS CONTROL

We maintain access control measures designed to limit access to our facilities and systems to a limited number of personnel who have a business need for such access. We ensure such access is removed when no longer required and conduct access reviews periodically.

## 10. ENCRYPTION

We encrypt all sensitive information in transit across public networks depending on the customer's requirement and ability to support encryption. Certain highly sensitive data is also encrypted at rest, including passwords as applicable.

## 11. RISK ASSESSMENTS

We have a documented risk management procedure and Secure Software Development Lifecycle process. We perform risk assessments of our products and infrastructure on a regular basis, application and infrastructure level testing for new products, and periodic reassessments of our network. We leverage access control, peer code review, as well as hardware and software protection against viruses being introduced into our systems or code. We have also taken measures to safeguard against data breaches and to detect any abuse. We use manual penetration testing and automated tools.

## 12. THIRD PARTY RISK ASSESSMENTS

We conduct security due diligence on third party service providers, which may include reviewing the scope of confidential information and personal data shared, a risk assessment of the service provider's organisation and technical security measures, the sensitivity of any information processed by the service provider, storage limitations, and data deletion procedures and timelines.

## 13. LEADERSHIP COMMITMENT

Our management team is committed to maintaining and continuously improving our information security standards and ensuring that these standards are met.