# Security Whitepaper

Grip.events

| | |
|---|---|
| Title | Security Whitepaper |
| Owner | Information Governance Management Team (GRIP) |
| Published Date | 08 March 2024 |
| Version | 3.0 |
| Document Classification | Public |

## Version history

| Version | Date | Updated By | Changes |
|---|---|---|---|
| 1.0 | 29.09.2021 | Information Governance Management Team (GRIP) | First Release |
| 2.0 | 26.05.2022 | Information Governance Management Team (GRIP) | Revised |
| 3.0 | 08.03.2024 | Information Governance Management Team (GRIP) | Revised |
| | | | |

# Table of Contents

# 1. Information Security Overview

## 1.1 Introduction

The security and integrity of Grip ("Intros.at" or "Company") information systems and technology infrastructure is important to enable the Company to operate its business and protect Company and client's information and assets.

Our CEO, and Directors ensure that information security is a top priority across the organisation.

## 1.2 information Security Framework

Our Information Security Management System ("ISMS") which is aligned with ISO 27001:2022, comprises policies designed to achieve and maintain the Grip's information security objectives, and to establish the minimum company-wide requirements for secure design, management, and operations of the Grip's information systems.

Our ISMS policies, govern and demonstrate management's commitment to safeguarding proprietary, confidential and personal information; provide direction and support for information security compliance with business requirements and relevant national and international laws and regulations; direct and benefit Company decision-making and incident response management; and are reviewed at planned intervals, or in response to significant business changes, to ensure continuing suitability, adequacy, and effectiveness of Grip's information security program.

The policies apply to all relevant parties, including company employees, independent contractors, consultants, suppliers/vendors, customers, and auditors, as applicable. All Grip's staff responsible for the design, build, management, operations, and security of the Company's computers, networks, and information systems are responsible for the implementation of and compliance with these policies.

Violations of the policies may result in corrective or other appropriate action, up to and including termination of employment or cancellation of contract(s).

# 2. Information Security Organisation

At Grip, we have an established Information Security Team dedicated to ensuring the security and integrity of the Company's systems and data, and the information we process on behalf of our customers. Through the deployment of security champions throughout the organisation, industry- recognized security tools, and a trained workforce in information security best practices, information security is embedded within the core of Grip's organisation and operations.

Our Information Security organisation comprises the following primary constituents:

## 2.1 Chief Technology Officer

Our CTO also serves as our acting Chief Information Security Officer. The Chief Technology Officer:

- Directs and manages our information security strategy.
- Champions our journey towards ISO 27001:2013 certification.

## 2.2 Information Engineering Team

- Promotes information security awareness.
- Maintains and advises on Information Security Policy.
- Develops and maintains security policies, standards and processes.
- Identifies and remediates global information security gaps
- Conducts vendor assessments and so participates in security audits
- Coordinates incident response and internal information security investigations.

# 3. Policy and Governance

Our policy and governance aligns with ISO 27001:2013 standards. The following topics are among those addressed by the Company's Information Security policies and procedures.

## 3.1 Asset Management

Grip has an asset management policy that identifies its assets and defines relevant protection responsibilities. Assets are assigned an owner and a custodian, and subject to an asset management lifecycle inclusive of on-boarding, management and decommissioning such as secure disposal or re-use.

### 3.2 Access Control

Physical and logical access to assets and systems is granted to individuals based on business and security requirements consistent with the following guiding principles:

- Need-to-know (access is only given if it is required to support a defined and documented business need)
- Least privilege (only the level of access strictly required is granted)
- Asset owner approval (each asset owner defines and approves who can access their assets)
- Segregation of duties (to reduce opportunities for unauthorised or unintentional modification or misuse of assets)

Identity and access management activities are defined to ensure the appropriate delivery of all types of access, and include the following processes:

- Access request, review and approval before granting access
- Regular review and recertification of access
- Revocation of access when it is no longer needed (user departure, business change, user re- assignment, termination of relationship with a customer, etc.)
- Maintenance of an audit trail of account creation, change and revocation

### 3.3 Information Classification

All information (physical or electronic form) that is processed, managed and stored by Grip is classified to ensure it receives an appropriate level of protection in accordance with its relative sensitivity.

### 3.4 Communication Security

Networks are managed and controlled to protect information in systems and applications. Network security management exists to ensure the protection of information in networks and its supporting information processing facilities.

Groups of information services, users, and systems are segregated as appropriate on networks through the use of domains and/or organisational units, and can be accomplished either physically or logically.

### 3.5 Information Security Incident Management

Management responsibilities and procedures are established to ensure a quick, effective, and orderly response to information security incidents.

### 3.6 Supplier Relationships

Security requirements are appropriately addressed and agreed upon within all supplier agreements, where the supplier may access, process, store or transmit Company or customer information, or may provide the Company with IT infrastructure components intended to do so. Agreements with suppliers include requirements to address the information security risks associated with information and communications technology and product supply chain.

### 3.7 Acceptable Use of Information Technology

At Grip, we have policies to guide all users on acceptable use of resources that have been available to them. Any individual who suspects incidents of misuse, fraud, loss and/or theft involving Company IT resources and/or information should immediately report the activity to his or her supervisor, manager, Human Resources department.

### 3.8 Business Continuity

At Grip, we ensure systems are well protected to ensure the resilience of critical business processes and we also have in place, technical disaster recovery and business continuity arrangements to minimise the business impacts of incidents.

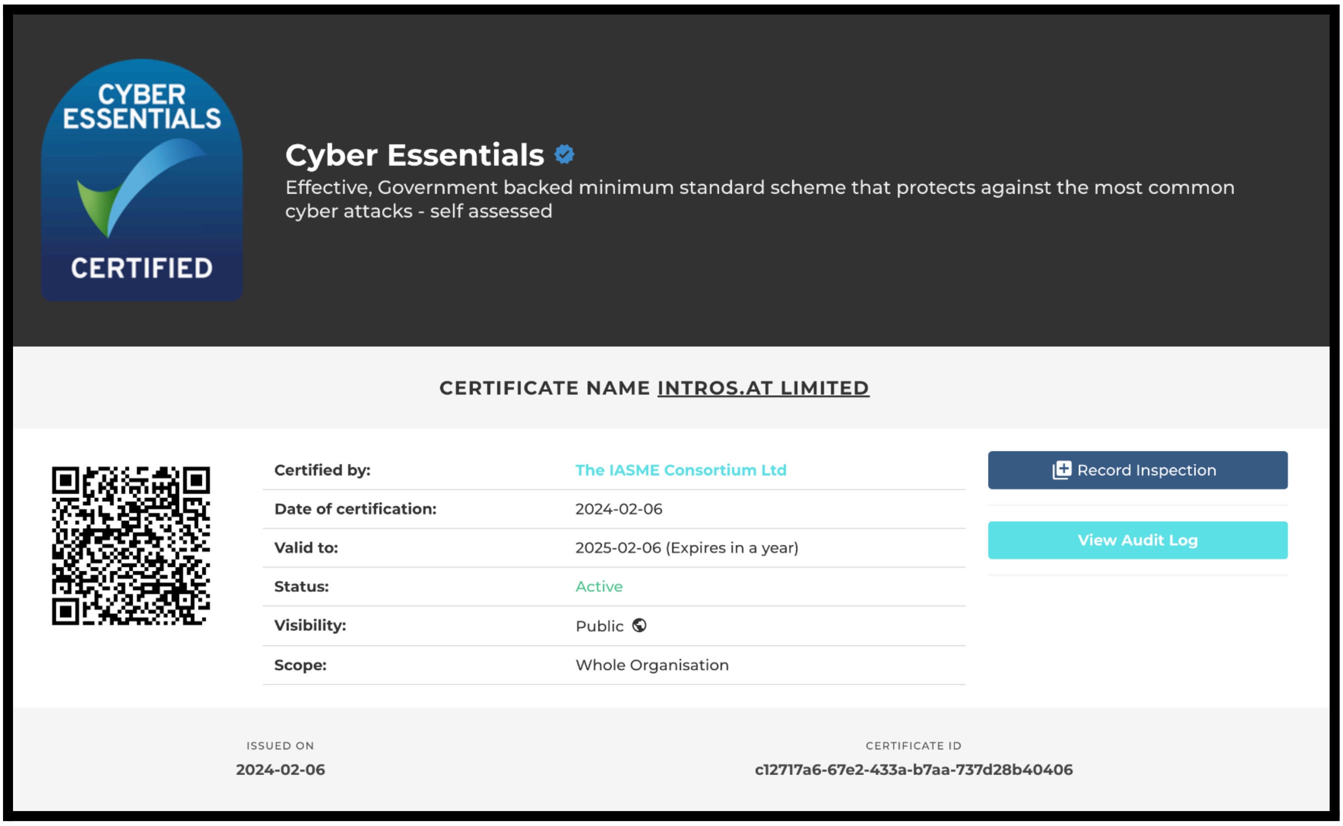
## Compliance With Standards

Grip engages accredited third parties to conduct Pentest on our test environment to provide assurance to Grip and its customers that adequate controls are in place to protect the confidentiality, integrity, and availability of all Company and customer sensitive data and assets.

Our practices are aligned with ISO 27001:2022 standard and we are also fully GDPR compliant.

We are accredited with the Cyber Essentials Certificate Scheme - a Government backed scheme which focuses on the important technical controls designed to protect against the most common cyber threats.

It demonstrates to clients that the most important basic cyber security controls are in place.



## Cyber Essentials

Effective, Government backed minimum standard scheme that protects against the most common cyber attacks - self assessed

CERTIFICATE NAME INTROS.AT LIMITED

| | |
|---|---|
| **Certified by:** | The IASME Consortium Ltd |
| **Date of certification:** | 2024-02-06 |
| **Valid to:** | 2025-02-06 (Expires in a year) |
| **Status:** | Active |
| **Visibility:** | Public |
| **Scope:** | Whole Organisation |

ISSUED ON
**2024-02-06**

CERTIFICATE ID
**c12717a6-67e2-433a-b7aa-737d28b40406**