POLICY

# Onclusive Information Security Policy

**Vishal Padhye (Document Owner)**
**2024 October Release**
**Public**

# TABLE OF CONTENTS

# Definitions

| Abbreviation | Definition |
|---|---|
| CEO | Chief Executive Officer |
| COO | Chief Operations Officer |
| CIO | Chief Information Officer |
| CISO | Chief Information Security Officer |
| ELT | Executive Leadership Team |
| ISMS | Information Security Management System |
| ISSM | Information Security State Manual |
| RACI | Responsible, Accountable, Consulted, and Informed |
| ISO/IEC 27001 | International Standard for Information Security Management, with the latest version as ISO/IEC 27001:2022 |
| PR | Public Relations |
| IS | Information Security |
| IS Org | Information Security Organization |

# 01. Mission Statement for Information Security at Onclusive Group

## 01.1 Commitment to Information Security

### 01.1.1

The Executive Leadership Team  of the Onclusive Group (ELT) fully commits itself to appropriately protecting the information of the Onclusive Group and that of our customers, employees, partners and supply chain.

As a world leader in media intelligence technology and services, we implement robust information and cyber security measures to protect our businesses around the globe. In doing so, we strive to prevent disruption of business operations, data theft and other related damage whilst ensuring compliance with laws and regulations in the countries in which we operate.

Securing and protecting information supports Onclusive's goal of achieving leading-edge innovation, human expertise and unmatched media reach in PR solutions. This policy also enables Onclusive to meet or exceed our customers' expectations and maintain our investors' trust, promoting growth in both existing and new markets, and to keep our employees' information private and secure.

## 01.2 Approach to information security

### 01.2.1

The ELT ensures that information security is promoted, implemented and managed consistently across the Onclusive Group by establishing a dedicated Information Security Organisation, which defines standards and supports processes, which are instantiated and implemented throughout Onclusive group.

At Onclusive, information security is based on:

- Ensuring adequate levels of protection by implementing appropriate governance, processes and technologies following a risk-based approach.
- Aligning all information security related activities to internationally recognized best practice and standards.
- Promoting continuous improvement of information security activities using our sentiment analysis methodologies.
- Engaging our employees as an essential part of our defence.

# 01.3 Governance of Information Security

## 01.3.1

The ELT has resolved that information security is governed through an Information Security Management System (ISMS) specified and documented in the Information Security State Manuals (ISSM) and is implemented across the Onclusive Group.

The Information Security State Manuals (ISSM) deliver a systematic approach to planning, adopting, implementing, supervising, and improving tasks and activities needed to protect information by leveraging people, processes, and information systems and by applying a risk management process. They address the following components:

1. Management of the Information Security Management System to ensure that all its parts are implemented across the group, to define information security requirements, and to ensure that the Information Security Organization functions appropriately.

2. Information Security Risk Management to identify, assess and mitigate risks and exploit opportunities using defined risk assessment criteria, and with unambiguously identified risk owners who approve the risk treatment plan and accept residual risk.

3. Information Security Measurement and Reporting to monitor, measure, analyse, and evaluate the effectiveness of the Information Security Management System. Metrics are used to improve the Information Security Management System and the technological environment, allowing management to make informed decisions.

4. Information Security Incident Management to ensure effective handling and communication of Information Security events and incidents, to resolve them in a timely manner with minimum disruption, to preserve evidence as required, and to improve capabilities, processes, and technologies from lessons learned.

5. Information Security Awareness, Education, Training, and Practise to enable our employees to properly identify and treat information security risks in the best interest of the Onclusive Group.

**The RACI Matrix is listed below: Responsible(R), Accountable (A), Consulted (C) and Informed (I)**

| Task / Activity | Responsible | Accountable (A) | Consulted (C) | informed (I) |
|---|---|---|---|---|
| Business Impact | (CEO) Chief Executive Officer | ELT ( Executive leadership Team | (COO) Chief Operations Officer | (CISO) Chief Information security officer |
| Information security policy Initiatives | (CIO) Chief Information Officer | (CEO) Chief Executive Officer | (CISO) Chief Information security officer | Information Security Team |
| Information security processes and procedures | Information security Steering Committee | (CISO) Chief Information security officer | (COO) Chief Operations Officer | (CIO) Chief Information Officer |
| Monitor information security Control | (CISO) Chief Information security officer | (COO) Chief Operations Officer | (CIO) Chief Information Officer | (CEO) Chief Executive Officer |

The financial, strategic, and operational needs of the Onclusive Group as well as legal and ethical standards determine our information security objectives. These objectives are measured to ensure that the intended goals are achieved within the appropriate timeframe.

# 02. SCOPE OF INFORMATION SECURITY

## 02.1 Control Set Reference

### 02.1.1

The ELT makes the voluntary commitment that the Information Security State Manual(ISSM) complies with International Standard Organization ISO/IEC 27001:2022.

## 02.2 Statement of applicability

### 02.2.1

Information security at Onclusive aims to protect all assets belonging to the Onclusive Group from information and cyber security related threats. This includes, but is not limited to, customer data, financial data, and employee data, applications, storage and computing devices, networks, and physical assets.

The Information Security State Manual (ISSM) is valid and binding for all personnel of the Onclusive Group and for suppliers and partners who must meet or exceed its requirements. The Information Security State Manual(ISSM) further addresses the information security requirements for customers, employees, government authorities, and public users.

## 02.3 Protection Objectives

### 02.3.1

Protecting against information security threats means preserving the confidentiality, integrity, and availability of information, which is understood as follows:

- **CONFIDENTIALITY**: Ensuring that information is accessible only to authorised individuals, entities or processes.

- **INTEGRITY**: Ensuring the accuracy and completeness of information over its entire lifecycle.

- **AVAILABILITY**: Ensuring that only authorised individuals, entities, or processes have timely and uninterrupted access to an information at all required times.

# 03. GUIDING PRINCIPLES OF INFORMATION SECURITY

## 03.1 Managing, Implementing and Supporting Information Security

### 03.1.1

These guiding principles define how to establish, implement, maintain, and continuously improve the Information Security Management System. The management team directly accountable for information security ensures that the Information Security Organization is and remains appropriately staffed with the required level of expertise and resources.

Information security roles and responsibilities are identified, defined, and established.

Employees of the Onclusive Group need to be aware of the Information Security State Manual(ISSM), how to support the Information Security Management System, the consequences of not implementing it. These awareness needs and all other information relevant to the successful implementation of the Information Security Management System need to be continuously communicated.

Suppliers and partners must ensure adequate and appropriate information security measures for the products and/or services that they provide. The required level of information security will be determined by means of a risk assessment, which is evaluated by members of the Information Security Organization.

## 03.2 Monitoring and Measuring the Effectiveness of Information Security

### 03.2.1

The effectiveness and efficiency of information security related activities inside and outside of the Information Security Management System are measured and monitored continuously with the support of appropriate methodologies and technologies.

Information security assessments, measuring effectiveness and efficiency, are performed following a defined plan that details scope, methodology, frequency, and entity.

The results of measurement and monitoring are duly analysed by the Information Security Organization, and provide input to management and may lead to technical, organisational, and procedural changes.

Effectiveness and efficiency of the Information Security Management System, as well as analysis and evaluation of the current risk level and of the threat environment, and the outcome of improvement and mitigation activities are reported to the ELT.

## 03.3. Operation of information security

### 03.3.1

Information is classified following a risk assessment approach and protected according to its classification.

Controls that mitigate risks are implemented in a timely manner and monitored to ensure their ongoing functioning and to support continuous improvement.

Information required to ensure the proper functioning of the Information Security Management System are collected, analysed in a timely manner, and reacted upon appropriately.

Changes to the Information Security Management System and subsequent documentation are identified and monitored to manage the required level of information security.

These changes are recorded, analysed, reviewed, and approved by the appropriate level of management and documented according to a standard process.

Information security events and incidents are treated appropriately by experts across the Onclusive Group.

## 03.4 Continuous improvement of Information Security

### 03.4.1

Following Onclusive's approach to continuous improvement, the Information Security Management System and subsequent documentation are reviewed annually and, if required, updated by a Information Security Committee.

The review takes into account significant changes to the external and internal context, the strategy of the Onclusive Group, and the results of relevant measurement and monitoring across the Onclusive group.

# REVISION HISTORY

| | |
|---|---|
| **Name** | Onclusive Information Security Policy |
| **Common Name** | ON-IS-PO-OCT-2024 |
| **Classification Level** | Public |
| **Governance Document Type** | Policy |
| **Owners** | Vishal Padhye |
| **Document Support** | Santhosh Kumar & Stanley Mugisha |
| **Reviewed by** | Robert Stone & Max Brierley-Jones |
| **Published** | 14/11/2024 |
| **Authorised** | (ELT) Executive Leadership Team |
| **Frequency of Review** | BI - Annually |