

TryHackMe

**ISMS SCOPE DOCUMENT**

|  |  |
| --- | --- |
| Code: | SCP-3301 |
| Version: | 0.4v |
| Date of version: | 01.04.2024 |
| Created by: | Paul Neko |
| Approved by: | Chirita Stanislav |
| Confidentiality level: | Confidential |

**Change history**

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Version** | **Created by** | **Description of change** |
| 2024-04-01 | 0.1 | Paul Neko | Schiță de bază a documentului |
| 2024-04-02 | 0.2 | Maria Ionescu | Adăugată secțiunea Introducere |
| 2024-04-03 | 0.3 | Ion Popescu | Adăugată secțiunea Concluzie |
| 2024-04-04 | 0.4 | Dejan Kosutic | Inserată bibliografie și formatare îmbunătățită |

**Table of contents**

[1. Purpose, scope and users 3](#_Toc415648235)

[2. Reference documents 3](#_Toc415648236)

[3. Definition of ISMS scope 3](#_Toc415648237)

[3.1. Processes and services 3](#_Toc415648238)

[3.2. Organizational units 3](#_Toc415648239)

[3.3. Locations 3](#_Toc415648240)

[3.4. Networks and IT infrastructure 3](#_Toc415648241)

[3.5. Exclusions from the scope 4](#_Toc415648242)

[4. Validity and document management 4](#_Toc415648243)

# Purpose, scope and users

The purpose of this document is to clearly define the boundaries of the Information Security Management System (ISMS) in TryHackMe.

This document is applied to all documentation and activities within the ISMS.

Users of this document are members of TryHackMe management, members of the project team implementing the ISMS, and Ben Spring, Ashu Savani .

# Reference documents

* ISO/IEC 27001 standard, clause 4.3
* **Project Plan for ISO 27001 Implementation**
* Produre for Identification of Requirements
* Law no. 133 of 8 July 2011 on the protection of personal data - This law regulates how personal data must be managed and protected. It is crucial for any cloud service that processes personal data of residents of Moldova.
* Law no. 71 of 22 March 2007 on the state register of legal acts - This law may contain relevant information about document management and electronic records, important aspects for cloud service providers.
* Law no. 284 of 22 July 2004 on e-commerce - It regulates issues related to e-commerce, including online transactions and their security, being relevant to cloud services that support economic online activities.

# Definition of ISMS scope

The organization needs to define the boundaries of its ISMS in order to decide which information it wants to protect. Such information will need to be protected no matter whether it is additionally stored, processed or transferred in or out of the ISMS scope. The fact that some information is available outside of the scope doesn't mean the security measures won't apply to it – this only means that the responsibility for applying the security measures will be transferred to a third party who manages that information.

Taking into account the legal, regulatory, contractual and other requirements, the ISMS scope is defined as specified in the following items:

## Processes and services

**Virtual Training Platform, Cybersecurity Labs, Platform Administration and Security**

## Organizational units

**Platform Administration Team, Customer Support Team, Content Creation Team, Development Team**

## Locations

**Headquarters, Data Centers, Remote Workspaces, User Locations.**

## Networks and IT infrastructure

**Internal Network, Production Network, Development and Testing Network, Customer Support Networ**

## Exclusions from the scope

The following is not included in the scope: **Third-party Services, User-Owned Devices, Physical Security Measures**.

# Validity and document management

This document is valid as of 2025-04-05.

The owner of this document is Ashu Savani , who must check and, if necessary, update the document at least once a year.

Exceptions for the update: In the event of significant events, such as malware attacks or natural disasters such as earthquakes, it is necessary to review and update the document immediately to address any changes in the risk profile and to integrate new security measures.

# Objectives

1. Ensuring data privacy: Protecting data against unauthorized access by implementing access control, data encryption at rest and in transit, and other security measures.
2. Data integrity: Ensuring that data is not tampered with. The implementation of checksums, digital likenesses and regular audits are essential to maintaining data integrity.
3. Service availability: Ensuring that cloud services and data are available to users when they are needed. This includes implementation of backup solutions, system redundancy, and robust business continuity and disaster recovery plans.
4. Risk management: Identifying, assessing and mitigating information security risks in a cloud environment. This may include regular risk assessments and the application of appropriate control measures to limit risks to an acceptable level.
5. Regulatory Compliance: Ensuring that the cloud service complies with relevant data protection laws and regulations, such as the GDPR in Europe. This includes implementing policies and procedures that support compliance.

Co-founders

Ashu Savani

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Ashu S.