

UNIVERSITY OF COPENHAGEN

SCIENCE HPC Center

(HPC@UCPH)

INFORMATION SECURITY POLICY

Version:	2.0.2
Date of version:	16.11.2026
Date of Approval:	18.11.2026
Created by:	Jonas Bardino, Jonas Bech Hansen, Aputsiak Niels Janussen, Trine Buhl Monty
Effective Date:	18.11.2026
Approved by:	Trine Buhl Monty
Confidentiality level:	PUBLIC

©2022 This template may be used by clients of Advisera Expert Solutions Ltd. www.advisera.com in accordance with the License Agreement.

Change history

Date	Version	Created by	Description of change
15.05.2018	1.0	Jonas Bardino	First official version
13.07.2018	1.1	Jonas Bardino	Updates based on suggestions from UCPH-ISO and UCPH-DPO. Minor corrections.
29.08.2019	-	Brian Vinter and Jonas Bardino	No changes, just annual review and approval
08.12.2020	1.2	Kenneth Skovhede and Jonas Bardino	Clarify management review participants. Political communication decisions belong with HPC-Lead rather than HPC-CISO.
16.12.2021	1.3	Jonas Bardino	Updated HPC-Lead.
16.02.2023	-	Jonas Bardino	No changes, just annual review and approval
21.11.2023 – 05.03.2024	1.5	Aputsiak Niels Janussen and Jonas Bardino	Transitioning from ISO 2013 to 2022 edition. Added document reference to Training and Awareness Plan. Change in HPC-Lead.
13.03.2025	-	Jonas Bardino	No content changes, just updated HPC-Lead and fixed different font on a few words in 4.2.
15.05.2025-21.05.2025	1.6	Aputsiak Niels Janussen	Included new Annual Cycle calendar document to the section Reference Documents. Inserted links to internally referenced ISMS documents. Edited full name for ANJ in “Created by”.
20.10.2025-05.12.2025	1.7	Aputsiak Niels Janussen	Updated clauses and control references.
17.03.2026-07.05.2026	2.0.0	Aputsiak Niels Janussen, Jonas Bardino and Jonas Bech Hansen	Updated entire document to accommodate feedback from ISO27001-certification audit about shortening and sharpening the information security policy and changing it to a public document.
22.05.2026	2.0.1	Jonas Bech Hansen	Updated information security objectives based on management review .

©2022 This template may be used by clients of Advisera Expert Solutions Ltd. www.advisera.com in accordance with the License Agreement.

28.10.2026-16.11.2025	2.0.2	Aputsiak Niels Janussen, Jonas Bardino, Jonas Bech Hansen and Trine Buhl Monty	Final editorial and content polish based on meetings and workshops.

©2022 This template may be used by clients of Advisera Expert Solutions Ltd. www.advisera.com in accordance with the License Agreement.

Table of contents

1. INTRODUCTION....5
2. REFERENCE DOCUMENTS....5
3. PURPOSE....5
4. SCOPE....5
5. APPLICABILITY....5
6. BASIC INFORMATION SECURITY TERMINOLOGY....5
7. INFORMATION SECURITY OBJECTIVES....6
8. MANAGEMENT REVIEW OF INFORMATION SECURITY....6
9. COMPLIANCE AND POLICY REQUIREMENTS....7
10. ISMS RESPONSIBILITIES....7
11. VALIDITY AND DOCUMENT MANAGEMENT....8

©2022 This template may be used by clients of Advisera Expert Solutions Ltd. www.advisera.com in accordance with the License Agreement.

1. Introduction

SCIENCE HPC Center at the University of Copenhagen (HPC@UCPH) is an organizational unit under the Faculty of Science (SCIENCE) at the University of Copenhagen (UCPH). HPC@UCPH is a mostly independent unit specializing in high-performance computing (HPC) and scalable solutions. It mainly supports research and teaching activities by providing secure and reliable high-performance computing, and services for storing, archiving and cross-organizational sharing of large datasets. HPC@UCPH focuses on digital sovereignty through open-source solutions and on-site hosting.

2. Reference documents

- ISO/IEC 27001 standard, clauses 5.2, 5.3, 6.1.1, 6.2, 7.4, 9.1, 9.3 and controls A.5.2, A.5.3, A.5.36, A.6.3
- Procedure for Document and Record Control (internal)
- ISMS Scope Document (internal)
- Risk Assessment and Risk Treatment Methodology (internal)
- Statement of Applicability (internal)
- List of Legal, Regulatory, Contractual and Other Requirements (internal)
- Data Breach Response and Notification Procedure (internal)
- Training and Awareness Plan (internal)
- Annual Cycle of ISMS Events & Activities (internal)

3. Purpose

This policy defines how HPC@UCPH protects information assets and ensures confidentiality, integrity, and availability in support of research and teaching activities. It also states our commitment to continuously improve our information security management system (ISMS) and maintain ISO27001-certification, while complying with applicable laws, including the EU General Data Protection Regulation (GDPR).

4. Scope

This policy applies to all activities, systems, and assets within the scope of the HPC@UCPH Information Security Management System (ISMS), covering research e-infrastructure and related services.

5. Applicability

Users of this document are all employees of UCPH assigned a role in the ISMS, as well as and relevant external parties, such as suppliers and cooperating partners with physical or logical access to HPC@UCPH's facilities, systems or data.

6. Basic Information Security Terminology

The ISMS takes a starting point in the following definitions:

- Confidentiality – characteristic of the information by which it is available only to authorized persons or systems.

©2022 This template may be used by clients of Advisera Expert Solutions Ltd. www.advisera.com in accordance with the License Agreement.

- Integrity – characteristic of the information by which it is changed only by authorized persons or systems in an allowed way.
- Availability – characteristic of the information by which it can be accessed by authorized persons when it is needed.
- Information security – preservation of confidentiality, integrity and availability of information.
- Information Security Management System – part of overall management processes that takes care of planning, implementing, maintaining, reviewing, and improving the information security.

7. Information Security Objectives

Within this framework, HPC@UCPH commits to Secure by Design and Secure by Default principles and aims at these high level information security objectives:

1. Confidentiality

- We provide e-infrastructure solutions to enable UCPH students, researchers and their collaboration partners to store, publish, share, and process their research and sensitive data, in compliance with applicable legislation, including GDPR.
- We limit data access to authorized users only and provide strong authentication and encryption of data in transit and at rest.

2. Integrity

- We protect user data against unauthorized modification and degradation through access control, hardware redundancies, remote backup, and end-to-end check-sums.
- We offer solutions to ensure that when published papers and data-sets are permanently archived, they are kept unalterable and intact according to scientific standards.

3. Availability

- We design and operate resilient, scalable services with built-in redundancy to ensure high service up-times and long-term data availability. This includes internal and external sharing of data with scientific peers and other collaborators.
- We take critical periods of UCPH user workload into consideration in the daily operations and maintenance of our services.

In addition to these high level information security objectives, top management may define shorter term strategic objectives and set specific performance goals in the periodic management reviews.

8. Management Review of Information Security

As a fundamental activity of the ISMS annual cycle, HPC-Lead, HPC-CISO and representatives of the steering committee for HPC@UCPH must review the information security at least once a year to establish the suitability, adequacy and effectiveness of the ISMS. This is also where the achievement of the information security objectives is evaluated and discussed in a strategic perspective. The evaluation is supported by the ISMS monitoring and performance results in the measurement report

©2022 This template may be used by clients of Advisera Expert Solutions Ltd. www.advisera.com in accordance with the License Agreement.

compiled by the ISMS Team as input to the review. Status on the fulfillment of past review decisions and the risk treatment plan as well as audit findings and corrective actions are also taken into account. Other recurring topics include changes in external or internal issues related to the ISMS or in the needs or requirements of interested parties. Based on the evaluation and discussions management decides and outlines overall plans and recommendations for the next period, along with performance and strategic goals. The outcome of the management review must be recorded in the management review minutes and relevant points communicated to the HPC@UCPH staff.

9. Compliance and policy requirements

9.1. General Information Security Requirements

This policy and the entire ISMS must be compliant with legal and regulatory requirements relevant to the organization in the area of information security and personal data protection, as well as with contractual obligations. HPC@UCPH maintains a detailed list of all contractual and legal requirements for that purpose in the List of Legal, Regulatory and Contractual Obligations.

9.2. Alignment with UCPH Information Security Policy

The ISMS of HPC@UCPH operates in full alignment with the general information security policy at UCPH. The principles of the UCPH policy serve as the mandatory security baseline for HPC@UCPH operations. Where HPC@UCPH extensions are stricter, they shall take precedence within the defined scope.

9.3. Information Security Controls

The process of selecting the information security controls (safeguards) is mainly risk-based as defined in the HPC@UCPH Risk Assessment and Risk Treatment Methodology. Objectives for individual security controls or groups of controls are proposed by HPC-CISO in collaboration with the employees involved in the daily operation. The selected controls and their implementation status are listed and approved by HPC-Lead in the HPC@UCPH Statement of Applicability.

10. ISMS Responsibilities

On an organizational level, the responsibility for the ISMS is divided in the following way:

- HPC-Lead is responsible for ensuring that the ISMS is implemented and maintained according to this policy, and for ensuring all necessary resources are available. HPC-Lead will define which information related to information security will be communicated to which interested party (both internal and external), by whom and when.
- HPC-CISO is responsible for operational coordination of the ISMS and personal data as well as for reporting about the performance of the ISMS. The latter includes setting and recording details about measurement methods, periodicities and results. HPC-CISO must ensure that all employees of HPC@UCPH, as well as appropriate external parties are familiar with this policy.

©2022 This template may be used by clients of Advisera Expert Solutions Ltd. www.advisera.com in accordance with the License Agreement.

- HPC-EM is responsible for adopting and implementing the Training and Awareness Plan, which covers information security training and awareness programs and applies to all persons with a role in the ISMS.
- The protection of integrity, availability, and confidentiality of assets is the responsibility of the owner of each asset.
- All data breaches, security incidents or weaknesses must be reported to HPC-Lead and other relevant entities in line with the Data Breach Response and Notification Procedure.
- All employees affiliated with HPC@UCPH must follow the ISMS policies and comply operationally with the guidelines and procedures for information security.

11. Validity and Document Management

This document is valid as of 18.11.2026.

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

When evaluating the effectiveness and adequacy of this document, the following criteria need to be considered:

- number of employees and external parties who have a role in the ISMS, but are not familiar with this document
- non-compliance of the ISMS with the laws and regulations, contractual obligations, and other internal documents of the organization
- ineffectiveness of ISMS implementation and maintenance
- unclear responsibilities for ISMS implementation

Signed off by:

HPC-CISO
Jonas Bardino

Approved on 18.11.2026 by:
HPC-Lead
Trine Buhl Monty

(Please refer to the *Procedure for Document and Record Control* for details on signing and approval)

©2022 This template may be used by clients of Advisera Expert Solutions Ltd. www.advisera.com in accordance with the License Agreement.