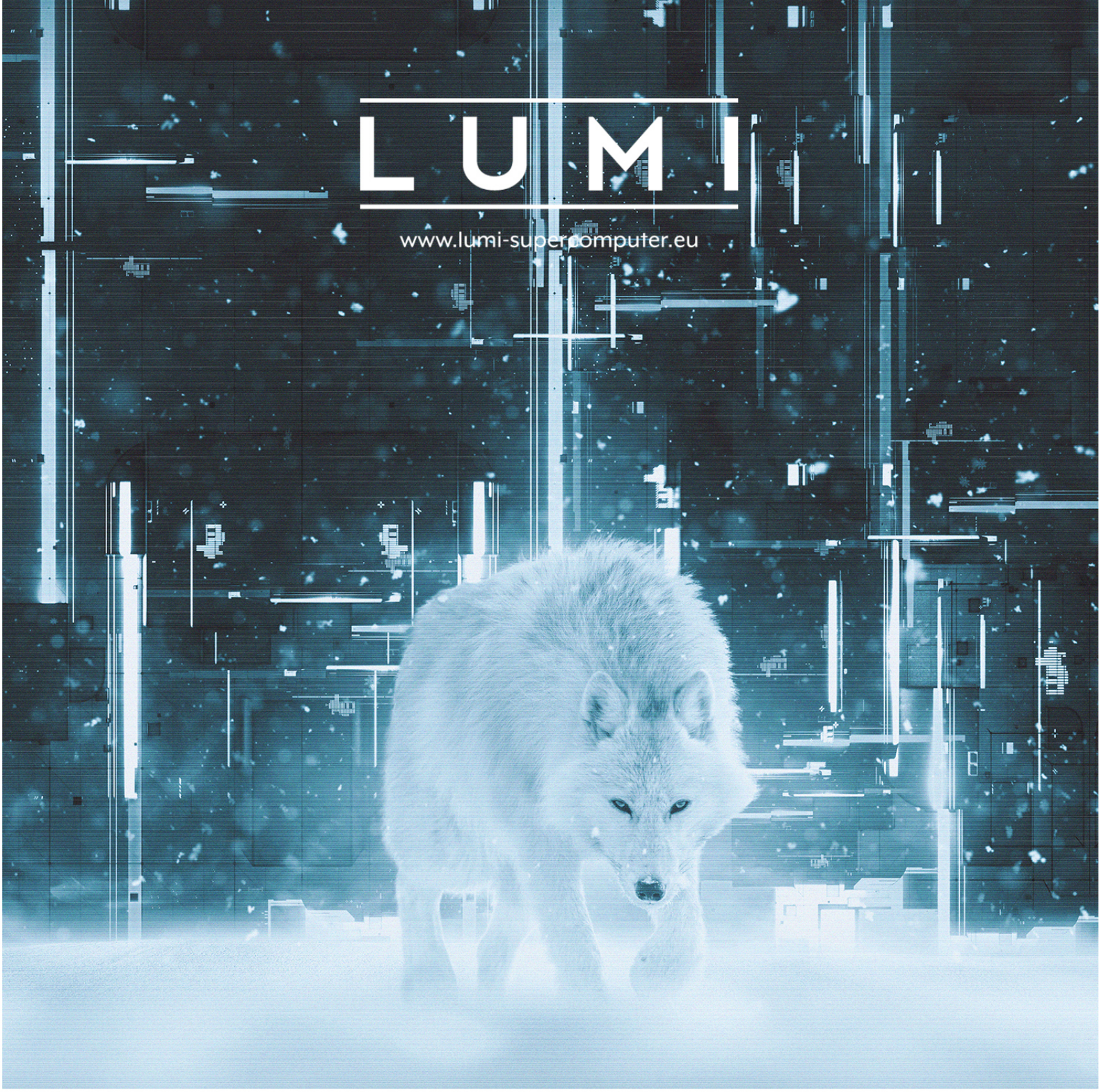

Cyber Security Statement

EuroHPC Joint Undertaking

The acquisition and operation of the EuroHPC supercomputer is funded jointly by the EuroHPC Joint Undertaking, through the European Union's Connecting Europe Facility and the Horizon 2020 research and innovation programme, as well as the of Participating States FI, BE, CH, CZ, DK, EE, IS, NO, PL, SE.

Leverage from the EU 2014–2020

European Union
European Regional Development Fund

REGIONAL COUNCIL OF KAINUU

EURO

LUMI

Cyber Security Statement for LUMI

Author(s)	Urpo Kaila & al.
Status	Approved
Version	1.0
Date	2021-09-14

Document identifier:	
Contributor(s)	Andreas Bach Stefan Becuwe Nicholas Cardo Nils Daniels Łukasz Flis Guy-Mael Horclois Le Pironnec Jarno Laitinen Torben Larsen Jakub Niezabitowski Juha Oinonen Michel Raes Tommy Tomson Lukas Vojacek
Reviewed by	Security SIG
Approved by	Strategic Committee
Dissemination level	Public

Quote

We aim to always find an optimal balance between security and usability based on risk management

EuroHPC Joint Undertaking

The acquisition and operation of the EuroHPC supercomputer is funded jointly by the EuroHPC Joint Undertaking, through the European Union's Connecting Europe Facility and the Horizon 2020 research and innovation programme, as well as the of Participating States FI, BE, CH, CZ, DK, EE, IS, NO, PL, SE.

Leverage from the EU 2014–2020

European Union European Regional Development Fund

REGIONAL COUNCIL OF KAINUU

EURO

Abstract:

This document is the Cyber Security Statement for the LUMI project and it sets the security principles that will be applied to protect the supercomputer environment, including user data and supporting services (for example Puhuri), hosted by the LUMI (Large Unified Modern Infrastructure) consortium.

Cyber Security Statement for LUMI

This document sets the security principles that will be applied to protect the supercomputer environment, including user data and supporting services (for example Puhuri), hosted by the LUMI (Large Unified Modern Infrastructure) consortium. Application of these security principles is responsibility of LUMI security and support teams.

LUMI, one of the EuroHPC pre-exascale supercomputers, is located at CSC's data center in Kajaani, Finland. The supercomputer is hosted by CSC for the LUMI consortium consisting of ten European countries as defined in the consortium and hosting agreements.

LUMI is an essential service for its stakeholders. LUMI will host vast amounts of academic and corporate research data.

LUMI strives to provide capabilities to process and store sensitive data.

Objectives

The objective of these security principles is to ensure the confidentiality, integrity, and availability of the services and data based on best international security practices and standards, risk management, and continuous improvement. Implementation of these principles will utilize state of the art security solutions balanced against the costs of implementation in relation to the risks and the nature of the data to be protected.

These principles will be applied in a resilient, transparent, and trust enabling manner with clearly defined roles for all stakeholders.

The objective of security measures is to support the mission of LUMI. Security is needed to ensure that the users and stakeholders of LUMI can transparently meet their security needs and requirements. By keeping

EuroHPC Joint Undertaking

The acquisition and operation of the EuroHPC supercomputer is funded jointly by the EuroHPC Joint Undertaking, through the European Union's Connecting Europe Facility and the Horizon 2020 research and innovation programme, as well as the of Participating States FI, BE, CH, CZ, DK, EE, IS, NO, PL, SE.

Leverage from the EU 2014–2020

European Union European Regional Development Fund

REGIONAL COUNCIL OF KAINUU

EURO

LUMI secure in an adequate and comprehensive way we can earn and maintain the trust of all our stakeholders.

We aim to always find an optimal balance between security and usability based on risk management, understanding the need for innovative and agile measures in the LUMI environment.

Scope

Although the security of the computing and storage platform is under responsibility of CSC (the hosting partner), user identification, authentication and authorisation, as part of resource allocation, is a distributed responsibility for LUMI consortium organisations and LUMI's partners, such as GÉANT, Tarto Puhuri Core and Puhuri Portal. This security strategy covers all functions as defined in the consortium agreement.

Liaisons

Due to the international nature of LUMI, security of LUMI will also constantly and closely liaise with European and international groups and frameworks for information security for research infrastructures, such as security initiatives by EOSC, PRACE security, WISE, GÉANT SIG-ISM, and related CSIRT communities.

To ensure the capability for incident response between LUMI partners, LUMI will operate a CSIRT team to handle incident coordination and crisis communication. LUMI CSIRT will apply SIRTFI incident response trust framework for incident coordination.

Security vulnerabilities will be proactively monitored and mitigated. LUMI will create procedures for the responsible disclosure of security vulnerabilities.

The LUMI operations teams are responsible to implement operational security measures according to security policy.

Applying security best practices

On specific security domains LUMI security will adhere to following approaches:

Key elements of LUMI Security Management are catalogues of operational resources to be protected, business continuity and disaster recovery plans, security agreements with customers and partners, a security awareness and skills training program, security guidelines, and an incident response procedure. Overall IT-Security is a responsibility also shared with all users and stakeholders of LUMI, and requires sufficient awareness creation, education and training.

EuroHPC Joint Undertaking

The acquisition and operation of the EuroHPC supercomputer is funded jointly by the EuroHPC Joint Undertaking, through the European Union's Connecting Europe Facility and the Horizon 2020 research and innovation programme, as well as the of Participating States FI, BE, CH, CZ, DK, EE, IS, NO, PL, SE.

Leverage from the EU 2014–2020

European Union European Regional Development Fund

REGIONAL COUNCIL OF KAINUU

EURO

Security is led by the role Head of Security.

Security measures are based on risk management and on classification of information.

LUMI physical Security is based on security zones, access controls and monitoring.

LUMI network and system security includes appropriate classification of networks, defence-in-depth, vulnerability scans, access controls, adequate encryption, logging and monitoring, ensuring availability, secure development, and change management.

LUMI security documentation is based on good governance and classification of data.

LUMI operations relies on procedures for IT service management including change, capacity, incident, and problem management.

Granting access to different roles in the LUMI environment is based on access management guidelines.

LUMI security measures aim to achieve compliance with applicable requirements, such as agreements and regulations which applies to LUMI and its stakeholders.

Compliance and reviews

To comply with data protection laws and data protection agreements, LUMI will implement appropriate technical and organisational measures.

LUMI hosting operations aim to comply with the ISO 27001 standard, and adapt forthcoming versions of the standard.

LUMI security procedures are regularly reviewed in internal and external audits and in management reviews.

Definitions

CSIRT Computer Security Incident Response Team

EOSC European Open Science Cloud

LUMI Large Unified Modern Infrastructure

PRACE Partnership for Advanced Computing in Europe

SIRTFI Security Incident Response Trust Framework for Federated Identity

WISE Wise Information Security for e-Infrastructures

EuroHPC Joint Undertaking

The acquisition and operation of the EuroHPC supercomputer is funded jointly by the EuroHPC Joint Undertaking, through the European Union's Connecting Europe Facility and the Horizon 2020 research and innovation programme, as well as the of Participating States FI, BE, CH, CZ, DK, EE, IS, NO, PL, SE.

Leverage from the EU 2014–2020

European Union European Regional Development Fund

REGIONAL COUNCIL OF KAINUU

EURO