Barcelona Supercomputing Center
Centro Nacional de Supercomputación

BSC-CNS Cyber Incident Management Policy

Version 1.0

Barcelona, 30th January 2024

Table of Contents

History

Date	Version	Changes	Owner
30/01/2024	1.0	Initial commit	Fernando Lopez Muñoz

1. Objective

The primary objective of this policy is to establish an effective framework for the management of cyber incidents to prevent, detect, respond, and recover from information security events at **Barcelona Supercomputing Center – Centro Nacional de Supercomputación (BSC-CNS).** This policy aims to ensure the confidentiality, integrity, and availability of critical information, as well as to minimize negative impacts on operations and the organization's reputation. Compliance with the provisions outlined in the **Real Decreto 311/2022, de 3 de mayo, which regulates the Esquema Nacional de Seguridad**, and adherence to the guidelines outlined in the **CCN STIC 817 guide**, will be integral to the implementation of this policy.

Additionally, it is essential to note that the regulatory framework to be followed is the security policy of **Barcelona Supercomputing Center – Centro Nacional de Supercomputación (BSC-CNS)**. The guidelines and directives outlined in the BSC-CNS security policy will be paramount in ensuring the effective execution of the measures outlined in this document."

2. Scope

This policy applies to all employees, contractors, suppliers, and third parties with access to **BSC-CNS**'s information resources. It includes both internal systems and those in cloud environments, as well as any device or network that may affect the organization's information security.

3. Guiding Principles

3.1. Prevention

Proactive measures, such as regular system and application updates, robust access policies, and physical security controls, will be implemented to prevent cyber incidents before they occur.

Ongoing staff awareness of current threats and best security practices will be an integral part of preventive measures.

3.2. Detection

Threat detection tools and processes will be implemented to identify cyber incidents promptly. This includes continuous monitoring of event logs, behavior analysis, and malware detection tools.

Regular audits will be conducted to assess the effectiveness of detection measures and ensure alignment with emerging threats.

3.3. Response

A Cyber Security Incident Response Team (CSIRT) will be established with well-defined roles and responsibilities. This team will coordinate responses to cyber incidents and ensure effective recovery.

Specific incident response plans will be developed and maintained to address different types of threats.

3.4. Recovery

Specific recovery plans will be developed for each identified type of cyber incident, ensuring a swift and secure restoration of affected services.

Regular drills will be conducted to assess the effectiveness of recovery plans and adjust them as necessary.

3.5. Collaboration

Collaboration with external organizations, such as government agencies and other industry entities, will be encouraged to share information on threats and tactics.

Active participation in security information-sharing communities will be maintained to stay informed about current threats.

3.6. Logging and Analysis

Detailed records of each cyber incident, including the cause, impact, and actions taken, will be maintained. This information will be valuable for improving the organization's security posture.

Post-incident analysis will be conducted to identify lessons learned and opportunities for continuous improvement.

3.7. Types of Incidents

The following types of incidents will be considered within the scope of this policy:

- Unauthorized Access Incidents
- Malware Incidents
- Denial of Service Incidents (DoS/DDoS)
- Information Leakage Incidents
- Security Flaw Incidents
- Fraud Incidents
- Resource Abuse Incidents
- Social Engineering Incidents
- Mobile Device Information Leakage Incidents
- Physical Security Incidents
- Non-Anonymized Information Detection Incidents

4. Roles and Responsibilities

4.1. Cyber Security Incident Response Team (CSIRT)

Coordinate responses to cyber incidents and ensure effective communication throughout the process.

Stay updated on emerging threats and best practices in incident management.

4.2. Information Security Officer

Oversee the implementation of security measures and coordinate with the CSIRT to effectively manage cyber incidents.

Notify relevant parties in case of incidents and provide periodic updates.

4.3. Users and Staff

Actively participate in security awareness and training programs.

Report any suspicious activity promptly to the CSIRT for a rapid response.

5. Notification and Communication

5.1. Internal Notification

Employees must promptly notify the CSIRT of any security incidents for a rapid and effective response.

5.2. External Notification

Notification of incidents to third parties will be conducted as required by relevant laws and regulations.

5.3. Communication of security incidents

In case of a cyber incident, the designated contact for the Cyber Security Incident Response Team (CSIRT) is the email address: security@bsc.es

In application of the General Data Protection Regulation, when a security incident occurs that constitutes a breach of the security of personal data, two types of communications must be considered:

• Communication with the Spanish Data Protection Agency.

• Communication to the affected data subjects, if deemed necessary and following applicable regulations.

In any case, regardless of the analyses conducted, the incident must be brought to the attention of the data subjects whose personal data is under the responsibility of the affected parties, BSC-CNS, in the event of a breach, providing information and also adhering to what is stipulated in the corresponding data processing agreements that may be signed regarding the responsibility for communicating incidents or security breaches.

To determine the need for communications, the Data Protection Officer of BSC-CNS (dpo@bsc.es) will consider the following factors:

- The volume of affected data:
  a. Value 1: Less than 100 records
  b. Value 2: Between 101 and 1,000 records
  c. Value 3: Between 1,001 and 100,000 records
  d. Value 4: Over 100,000 records
  e. Value 5: More than 1,000,000 records

- Type of affected data:
  a. Value 1: Non-sensitive data
  b. Value 2: Sensitive data

- Impact (Exposure):
  a. Value 2: None
  b. Value 4: Internal, within the entity, controlled.
  c. Value 6: External
  d. Value 8: Public, accessible on the internet
  e. Value 10: Unknown

Once the above factors are determined, the Security Officer and the Data Protection Officer proceed to calculate the risk of the security breach according to the following formula:

Risk = Volume x Type x Impact

The following communication policy is applied:

- Communication to the Spanish Data Protection Agency when the following two conditions are met:
  - Risk exceeds 20. o
  - Two or more of the following circumstances occur:
    - More than 100,000 records are affected.
    - Personal data is affected.
    - The impact is external, public, or unknown.
- Communication to the data subjects when the following two conditions are met:
  - Risk exceeds 40.
  - Two or more of the following circumstances occur:
    - More than 25 records are affected.
    - Data of special categories is affected.
    - The impact is external, public, or unknown.

Communication to the Spanish Agency in the role of the Supervisory Authority If the conditions mentioned above are met, the Data Protection Officer will notify the security breach to the competent data protection supervisory authority without undue delay and, at the latest, within 72 natural hours after becoming aware of it. The notification to the competent data protection supervisory authority will be made following its instructions.

Communication to the affected data subjects If the conditions mentioned above are met, the Data Protection Officer of BSC-CNS will manage the communication to the affected data subjects without undue delay, providing the following information:

a. Identification and contact details of the data protection officer or another contact point where more information can be obtained.
b. Description of the possible consequences of the breach of the security of personal data.
c. Description of the measures taken or proposed by the data controller to remedy the breach of the security of personal data, including, if applicable, measures taken to mitigate possible negative effects.

Communication with the data subjects will not be necessary if any of the following conditions are met:

a. Adequate technical and organizational protection measures have been implemented and applied to the personal data affected by the breach, especially those that make the personal data unintelligible to anyone not authorized to access them, such as encryption.
b. Further measures have been taken to ensure that there is no longer a probability that the high risk to the rights and freedoms of the data subject will materialize.
c. It involves a disproportionate effort. In such a case, public communication or a similar measure will be opted for, equally effectively informing the data subjects.
d. The security breach cannot cause significant harm to the affected data subjects. However, this communication must be carried out in a coordinated manner with the affected parties of BSC-CNS.

6. References

Real Decreto 311/2022, de 3 de mayo por el que se regula el Esquema Nacional de Seguridad

CCN STIC 817 - Guía para la Gestión de Ciberincidentes

7. Reviews and Updates

This policy will be reviewed periodically to ensure its relevance and effectiveness, taking into consideration updates to the Esquema Nacional de Seguridad and CCN STIC 817 guidelines. Updates will be made to reflect changes in the threat landscape and best practices in cyber incident management. The policy will be reviewed at least once a year, or more frequently if significant changes in infrastructure or threats are identified.

This policy is a living document, and all members of the organization are expected to review and understand it. Adherence to this policy is essential to ensure the ongoing security of information at **BSC-CNS**.