genenta science

STANDARD OPERATING PROCEDURE

GEN-CORP-SOP-035 v1.0

TITLE

CYBERSECURITY INCIDENT MANAGEMENT PROCESS

Supersedes:	Not Applicable	Effective Date:	2024.06.15
Author:	Mattia Campagner, CISO	DocuSigned by: Mattia Campagner EA197E971B5E4E8... ....Signature/Date	
Reviewed by:	Barbara Regonini, Finance Director	DocuSigned by: Barbara Regonini F6D6D5BC13D2447... ....Signature/Date	
Reviewed by:	Richard Slansky, Chief Financial Officer	DocuSigned by: Richard Slansky 067339D583F946F... ....Signature/Date	
Approved by Management:	Pierluigi Paracchi CEO	DocuSigned by: EDABBB17C210458... ....Signature/Date	

Effective Date: 2024/06/15

TABLE OF CONTENTS

PAGE

Effective Date: 2024/06/15

1. PURPOSE AND SCOPE

The purpose of this document is to describe the process of managing security incidents that may impact the Company's systems, networks and devices, defining organizational and operational procedures based on structured phases with activities, classifications and taxonomies that are clear and shared.

From a security perspective, the procedures are aimed at maintaining and, following any breach, restoring information security, establishing in a timely manner the actions to be taken in the event of a possible security incident, with the aim of minimizing its impacts and learning the lessons deriving from their occurrence with a view to continuous improvement.

This SOP applies to Genenta Science S.p.A. and Genenta Science, Inc. (both and separately "the Subsidiaries") and Genenta Science S.p.A. as the Consolidating Parent Company ("the Company" or "Genenta").

2. OBJECTIVE

This standard operating procedure ("SOP") aims to define and describe an action plan including the methodologies to be applied to support the Information Security Incident Management ("ISIM") process.

This process addresses:

- Monitoring security events and their transition to security incidents.
- Controlling security incidents through incident resolution.
- Complying with regulatory obligations in terms of communication and transparency in case of incidents.
- Leveraging lessons learned for process improvement.

The ISIM action plan aims to monitor the Genenta computing environment and respond proactively throughout the lifecycle of security incidents which is composed of six (6) phases:

- Incident Detection
- Incident Assessment
- Incident Containment
- Incident Eradication
- Incident Recovery
- Post-incident Review

This plan shall apply to all systems that process, handle, or transmit Genenta data in any form, and any data that is in transit or at rest on Genenta systems.

Section 6 of the SOP is dedicated to describe the reporting process in case of material cybersecurity incident.

3. DEFINITIONS

- An **event trigger** or **cybersecurity threat** is any potential unauthorized occurrence on or conducted through a Company's information systems that may result in adverse effects on the confidentiality, integrity or availability of the Company's information systems or any information residing therein. It refers to any event that can activate a security response and that might require security personnel's attention.

- A **cybersecurity incident** is an unauthorized occurrence, or a series of related unauthorized occurrences, on or conducted through a Company's information systems or any information residing therein.
- A **material cybersecurity incident** is a significant security breach or event that has a substantial impact on an organization's operations, data, or reputation, often requiring specific reporting and response actions due to its significance.
- An **incident responder** is the subject that first starts the analysis of the event that is deemed to be a security incident. Typically, she/he is the IT Manager or an internal referent for an external service.

4. ROLES AND RESPONSIBILITIES

The subjects involved in the process are as follows:

Security Committee: the Security Committee is made up of the Finance Director, the IT Manager, and the Chief Information Security Officer ("CISO")

Chief Information Security Officer: the CISOis responsible for overseeing the implementation and management of comprehensive information security programs to protect the organization's assets from potential threats and breaches.

Security Information and Event Management: the responsibility of Security Information and Event Management ("SIEM") is to collect, analyze, and correlate security event data from various sources to detect and respond to security threats effectively.

IT Manager: the IT manager supports the CISO in audit activities, remains updated on cybersecurity developments and legal implications, ensures the application of minimum-security standards, reports non-compliance to the Security Committee, suggests software solutions to the Security Committee, collaborates on corrective action plans and advises on the initiation, modification, or termination of IT security projects.

Incident Responder: the incident responder performs the first analysis of the event and to involve the CISO if a security incident is suspected.

Users: Genenta users are employees, contractors, and service providers.

The roles and responsibilities of the parties involved in the process are further defined on a phase-by-phase basis according to the RACI matrix (see below).

The **RACI matrix** is a project management tool used to clarify roles and responsibilities within a project or organization by defining who is responsible, accountable, consulted, and informed for each task or decision.

R - Responsible: the individual or group responsible for completing the task or making the decision.
A - Accountable: the individual who is ultimately answerable for the task or decision.
C - Consulted: individuals or groups whose input is sought before a decision or action is taken.
I - Informed: individuals or groups who need to be kept informed about the progress or outcome of a task or decision.

See **section 6** of this SOP for the ISIM process summary table.

5. PROCESS

Process Frequency: As needed.

5.1. DETECTION

5.1.1 Input

The process input is an event trigger contained within any process activity from multiple potential sources, such as:

- **Cisko Meraki:** The Cisco Meraki application is a cloud-based management platform that centrally configures, monitors, and controls Cisco Meraki networking and security devices from a single dashboard.
- **Cisco Umbrella DNS Advance**: The Cisco Umbrella DNS Advantage application is a cloud-delivered security service that provides advanced threat protection, secure web gateway functionality, and DNS-layer security to protect users and devices from malware, phishing, and other internet threats.
- **Microsoft Defender Endpoint:** The Microsoft Defender Endpoint application is an advanced endpoint security solution that protects devices from cyber threats, detects and responds to attacks in real time, and helps secure networks against sophisticated attacks.
- **Microsoft Defender Cloud for App**: Microsoft Defender for Cloud Apps is a comprehensive cloud access security broker (CASB) solution that helps organizations protect their cloud-based applications and data from threats, compliance risks, and data breaches.
- **CyberHunter SIEM/SOAR**: The CyberHunter SIEM/SOAR application is an integrated security information and event management ("SIEM") and security orchestration, automation, and response ("SOAR") platform that enables organizations to detect, investigate, and respond to security threats efficiently and effectively.
- **Cybersonar CTI:** The Cybersonar CTI application is a cyber threat intelligence platform that provides organizations with real-time insights into cyber threats, vulnerabilities, and risks, enabling proactive defense and response measures.
- **Genenta Users**: Employees, contractors, and service providers reporting.

5.1.2 Activity

Employees, contractors, and service providers shall notify the IT Manager of any anomaly that they might notice in any operating system functionality that might represent a trigger event.

A trigger is merely an indication of a security event warranting (alert) further investigation.

All data collected by any source in the system have a predefined suspicious event trigger.

The event is first analyzed by the Incident Responder to understand if it can be connected to a security incident. In that case, the CISO is involved in the analysis. Security incidents analysis passes to the assessment phase, while "near miss" events are recorded in the IT Ticketing system.

5.1.3 Output

An incident record serves as the record for the process.

5.1.4 Process controls

ORGANIZATIONAL CONTROLS			
Role	**Responsibilities**	**Authority**	**Qualifications**
IT Manager/ Incident Responder	Determine whether knowledge of alert detector notice exceeds alert threshold levels	• Read sensor warnings	• Knowledge of alert thresholds
CISO	Determine whether warning merits further response	• Take command of the incident and assign it to next process	• Knowledge of alert thresholds • Ability to direct resources as needed

OTHER PROCESS CONTROLS			
Physical	**Technical**	**Procedural**	**Governance**
The physical perimeter of the defined domain	Activity sensors	• Domain definition • Suspicious activity warning • Alert thresholds • Alert response	• Incident record

5.2. ASSESSMENT

Process Frequency: As needed.

5.2.1 Input

The input for this process is an incident record generated by the Incident Detection Process.

5.2.2 Activity

The CISO, after consulting the Security Committee will:

1. **Validate the Incident Record and conduct an impact analysis on the affected areas.**
   a. If the Alert is invalid, the process flow returns to the Incident Detection process.
   b. If the Alert is valid the process flow continues.

2. **Categorize the Incident type such as:**

   - Denial of service/DDoS
   - Technical intrusion
   - Presence of malware
   - Social Engineering/Phishing/Spear Phishing
   - Ransomware
   - Web-based attack
   - Data Breach
   - Websites defacement
   - Third-party security incident (customer/service provider)

- Elevation of privilege
- Resource used for illicit purposes
- Disclosure of information
- Other (specify)

Further details of incident types are in Annex 2.

3. The CISO involves the appropriate stakeholders (e.g., head of the impacted corporate function), including the members of the Security Committee, to assess the impact and the materiality (together "the severity") and assign to the incident a severity level.

a. <u>The severity assessment is performed considering a combination of qualitative and quantitative factors, which may include:</u>

I. Data Sensitivity: the type and sensitivity of data exposed or compromised, such as personal or financial information.

II. Volume of Data: the amount of data affected, which can impact the severity of the incident.

III. Regulatory Impact: the potential regulatory consequences and legal obligations arising from the incident, including fines and penalties.

IV. Reputation Damage: the harm to the Company's reputation which can lead to stakeholders' attrition and loss of trust.

V. Financial Impact: the direct financial costs related to the incident, such as incident response, recovery, and potential lawsuits.

VI. Operational Disruption: the extent of disruption to normal business operations and productivity.

VII. Market Reaction: how investors, analysts, and the market respond to the incident, affecting stock price and market capitalization.

VIII. Insurance Coverage: the extent to which insurance coverage may mitigate financial losses.

IX. Long-Term Effects: consideration of the long-term effects on the organization, including the potential for recurring incidents.

X. Third-Party Relationships: assessment of the impact on relationships with partners, suppliers, and vendors.

b. <u>The criteria above mentioned leads to the assignment of the severity level:</u>

I. **Sev 5:** Worst Case business impact:

Catastrophic and complete operational failure. "Bet the farm impact:" not surmountable situation. Catastrophic damage to organizational assets, significant financial loss, or catastrophic harm to individuals that may include loss of life or serious life-threatening injuries.

II. **Sev 4**: Severe business impact:

Severe loss of operational capability, highly damaging and extremely costly but survivable.

III. **Sev 3:** Major business impact:

Substantial operational impact, to the extent that the organization is unable to perform one or more of its primary functions.

IV. **Sev 2:** Moderate business impact:

Noticeable but limited operational impact, to an extent and duration that the organization can perform its primary functions, but the effectiveness of the functions is significantly reduced; some costs.

V. **Sev 1**: Minor business impact:

Minimal, if any, operational impact: to an extent and duration that the organization can perform its primary functions but the effectiveness of the functions is noticeably reduced.

The final severity score is calculated as the average score of all scores assigned to each item listed above, rated from 1 to 5, where 1 represents the lowest impact and materiality, and 5 represents the highest.

If the incident severity level is between 5 (Worst Case) and 3 (Major), a Crisis Management Team shall be formed. The CEO (or delegate) will chair the team and may also nominate contributors to the Security Committee other than the Finance Director, the IT Manager, and the CISO as, for instance third-party experts and consultants. The BoD and the Data Protection Officer (“DPO”) shall be informed.

The CISO, involving the appropriate stakeholders, draws the initial action plan.

Then she or he defines the internal incident communication protocols (e.g., Crisis Management Team meets every day at a defined time, etc.). The communication protocols are applied during all the phases of the incident management.

The CISO will supervise the tracking of all the activities in the incident management phases.

5.2.3 Output

The fully defined Incident Alert is the output and serves as a record. Other activities related to the process, including Containment, Eradication, and Recovery actions to be implemented should be documented and added to the incident records as needed. In case of a material incident with a severity level between 5 (Worst Case) and 3 (Major), a reporting and communication process starts in compliance with the SEC regulation applicable to public Companies. Please refer to S**ection 6.1**

5.2.4 Process Controls

ORGANIZATIONAL CONTROLS			
Role	**Responsibilities**	**Authority**	**Qualifications**
CISO	Impact analysis and affected areas	• Categorize and prioritize security alerts • Assignment of response tasks	• Knowledge of incident categories • Knowledge of incident severity levels
CISO	Formalization of the action plan	• Action plan	• Reporting

OTHER PROCESS CONTROLS			
Physical	**Technical**	**Procedural**	**Governance**
None	None	• Category definitions • Priority definitions	• Fully defined Incident Alert

			• Related incident activity records

5.3. CONTAINMENT

Process Frequency: As needed

5.3.1 Input

The input for this process is a fully defined Incident Alert from the Assessment process issued by the CISO.

5.3.2 Activity

The CISO takes the coordination of the activities to involve the appropriate stakeholders to perform containment activities, which include:

- Isolate the Threat: the primary goal is to isolate the affected systems or devices to prevent the threat from spreading to other parts of the network. This might involve disconnecting infected machines, restricting network access, or disabling compromised accounts.
- Stop the Attack: actions are taken to halt the ongoing attack itself. This could involve stopping malicious processes, patching vulnerabilities, or filtering out malicious traffic.
- Preserve Evidence: any evidence related to the incident needs to be preserved for potential investigation and forensic analysis. This might involve collecting logs, system snapshots, and other relevant data.
- Minimize Damage: efforts are made to minimize the overall impact of the incident. This could involve stopping data exfiltration, restoring backups, or implementing mitigation strategies.
- Document the Activities: document all actions taken during containment for future reference and improvement of the incident response process. This includes the timeline of events, containment steps, and personnel involved.
- Communication Plan: an internal and external communication plan highlights all the needed communication flows, with relevant stakeholders and with authorities (including law compliance, e.g., Data Protection authorities, Form F-6K to SEC within 4 business days).

Based on the severity value assigned during the Assessment Phase the Security Committee might define additional solution strategies determining the affected zone and isolation options within the affected security domain.

When applicable, the Crisis Management Team is kept updated to be able to provide guidance and approvals.

5.3.3 Output

The output will be a Containment Confirmation Notice included in the incident report. The output will serve as a record of the process.

5.3.4 Process Controls

ORGANIZATIONAL CONTROLS			
Role	**Responsibilities**	**Authority**	**Qualifications**
Security Committee	Definition of response initiatives	• Definition of possible solution strategies	• Knowledge of relevant network • Segments and/or devices
Security Committee	Execution of response initiatives	• Execution of organizational, technical, and communication related measures as required	• Knowledge of relevant network segments and/or devices

OTHER PROCESS CONTROLS			
Physical	**Technical**	**Procedural**	**Governance**
Physical perimeter of defined domain	• Network topology • System management tools	• Security Domain definitions • Response playbooks	• Containment Confirmation Notice • User Account Change Request • Related incident activities to be reported

5.4. ERADICATION

Process Frequency: As needed.

5.4.1 Input

The input for this process is an Incident Alert from the Assessment and/or Containment process which indicates the threat originated as malware, as an attack on a vulnerability, or is of similar malicious intent and the actions that should be implemented in this phase.

5.4.2 Activity

1. The Security Committee, after consultation with appropriate stakeholders, formulates a hypothesis of technical and organizational eradication measures. When applicable, eradication measures are submitted to the Crisis Committee for approval.

   i. Determine if the incident originated internally or external to the domain.

      a. If external, the IT Manager as incident responder should close access to the domain from the outside to prevent further attack.
      b. If internal, determine whether the basis is corrupt software (if so, restore the approved software), a software vulnerability (if so, perform an emergency patch process, if no patch exists, the CISO together with the IT Manager, will determine an appropriate compensating control e.g., manual monitoring), some other potential vulnerability (if so, research the vulnerability and if necessary, replace the affected device).

2. The CISO will coordinate activities to define the eradication plan, assigning activities, and agreeing to target timing. Then s/he will perform and monitor the execution of organizational and technical eradication measures, which include:

i. Identify Root Cause: a thorough investigation is conducted to determine the root cause of the incident. This helps prevent similar incidents from happening in the future.
ii. Eradicate the Threat: once the root cause is identified, steps are taken to remove the threat entirely. This might involve removing malware, patching vulnerabilities, or reconfiguring compromised systems.
iii. Review and Update Security Measures: security configurations and policies are reviewed and updated to address the vulnerabilities exploited in the incident. This helps strengthen the overall security posture and prevent future attacks.
iv. Test Systems: eradication efforts are validated by testing the systems to ensure the threat has been completely removed and normal functionality is restored.
v. Prepare for Recovery: the groundwork is laid for the recovery phase, which involves restoring affected systems and data. This might involve preparing backups, verifying data integrity, and developing a recovery plan.

3. Finally, the CISO will:
   vi. Evaluate the adequacy of the effort in achieving eradication.
      a. If inadequate, return to the Incident Responder or the appropriate stakeholder for follow-up.
      b. If adequate, issue an Eradication Confirmation Notice.
   ii. Evaluate whether remediation is required.
      a. If yes, proceed to the remediation process.
      b. If no, proceed to the Post-Incident Review process.

4. Update incident records to reflect activity.

5.4.3 Output

1. Eradication Confirmation Notice
2. Updated incident record

One or both outputs will serve as a record for this process.

5.4.4 Process Controls

ORGANIZATIONAL CONTROLS			
Role	**Responsibilities**	**Authority**	**Qualifications**
CISO	Definition of additional eradication measures	• Segment / Platform / Application / Process shutdown as required • Administrative access as required	• Knowledge of relevant network segments and/or devices
IT Manager/CISO	• Execute organizational eradication • Execute technical eradication	• Segment/platform/application/process shutdown as required • Administrative access as required	• Knowledge of relevant network segments and/or devices
CISO	• Determine the adequacy of eradication and the next steps to take	• Evaluate eradication efforts • Determine appropriate next steps	• Knowledge of relevant network segments and/or devices

			• Knowledge of response playbooks • Ability to direct response activities

OTHER PROCESS CONTROLS

Physical	Technical	Procedural	Governance
None	• Software patches or updates • Administrative access to devices	• Response playbooks • Standard Operating Procedures for devices	• Eradication Confirmation Notice • Updated incident record

5.5. RECOVERY

Process Frequency: As needed.

5.5.1 Input

The input for the process is a remediation requirement from the Assessment and/or Eradication process.

5.5.2 Activity

The CISO, together with the IT Manager will:

1. Prioritize the requirement for business criticality, Recovery Time Objective (“RTO”), and Recovery Point Objective (“RPO”).
2. If the recovery requires hardware deployment:
    a. Determine the hardware needed based on system hardware specification.
    b. Acquire new or retrieve repurposed hardware as needed.
    c. Retrieve the required system configuration from the system specifications.
    d. Remove, replace, and configure the hardware.
    e. Submit the restored hardware for system evaluation.
3. If the recovery requires software deployment:
    a. Establish the recovery point based on the RPO specified for the software.
    b. Retrieve the required software, whether from original or backup media.
    c. Retrieve the data required to match RPO from backup media.
    d. Reload the software.
    e. Restore data to the system.
    f. Submit the restored system for system evaluation.

The IT Manager together with the CISO will:

1. Evaluate the restored systems for conformance to the system acceptance criteria.
    a. If the restored systems are found inadequate, return the task to the IT Manager for follow-up.
    b. If the restored systems are adequate, issue a Recovery Confirmation Notice.
2. The CISO, after consulting the Security Committee, defines an improvement plan outlining the extra costs.
3. The improvement plan must be submitted to the Senior Management Team and, as appropriate, to the BOD for approval based on the materiality of the plan in term of costs.
4. The Recovery and the improvement plan approved becomes part of the incident record.
5. Update incident records as needed.

5.5.3 Output

The output is the Recovery Confirmation Notice and the updated incident record. Both outputs may serve as records of this process.

5.5.4 Process Controls

ORGANIZATIONAL CONTROLS

Role	**Responsibilities**	**Authority**	**Qualifications**
IT Manager/Incident Responder	Participation in response initiatives	• Execution of response playbooks • Segment/Platform/Application/ Process shutdown as required. • System changes without prior Change Management approval • Administrative access as required	• Knowledge of relevant network segments and/or devices
IT Manager/Incident Responder	Evaluate remediation adequacy	• Evaluation of system against defined criteria • Decision authority to proceed with deploying to production	• Knowledge of system acceptance criteria • Knowledge of domain recovery specifications

OTHER PROCESS CONTROLS

Physical	**Technical**	**Procedural**	**Governance**
Definition of physical domain boundaries	• System specifications • RTO/RPO specifications	• Domain Recovery Specifications • Response playbooks • Device Standard Operating Procedures • System Acceptance Criteria	• Remediation Confirmation Notice • Updated incident record

5.6. POST-INCIDENT REVIEW

Process Frequency: As needed

5.6.1 Input

The input for this process is an incident report, which may result from any of the Containment, Eradication, or Remediation process or from all these processes.

5.6.2 Activity

The CISO will perform incident review analysis and determine whether the incident analysis requires forensic review. In this case:

- Gather any available incident logs and records;
- Gather data about or from the system(s) affected; and,
- Analyze the incident per the forensic analysis procedure (evaluation to involve specific consultants for forensics activities will be performed, involving the appropriate stakeholders).

Once the main activities have been restored, a "lesson learned" meeting will be organized to evaluate the incident and implement the strategies, policies and procedures necessary to avoid the recurrence of similar incidents.

In particular, the purpose of this meeting will be to give an answer to the following questions:

- What happened and when?
- What was done to handle the incident (were procedures followed)?
- What information would have been useful to detect the incident in time?
- Have there been any actions that have made the situation worse?
- What will we do differently the next time such an incident occurs?
- What actions can prevent similar incidents?
- What clues will help us to detect similar incidents in the future?
- What tools or resources do we need to detect and stop future incidents?

The CISO will:
1. Review the Incident Analysis Report
2. The results will become a part of the incident database for future reference.

5.6.3 Output

The approved Incident Analysis Report serves as the output of this process.

5.6.4 Process Controls

ORGANIZATIONAL CONTROLS

Role	**Responsibilities**	**Authority**	**Qualifications**
CISO	Analysis of forensic or performance issues in incident record	• Incident Analysis Report • Administrative access as required	• General knowledge of security threats • Ability to analyze incidents for root cause, • remediation methods, and lessons learned
CISO	Review and approval of Incident Analysis Report	• Report approval	• Ability to analyze incidents for root cause, • remediation methods, and lessons learned
CISO	Drafting an improvement plan (extra costs)	• Explain the specific extra costs	• Knowledge of domain recovery specifications • Knowledge of system acceptance criteria

OTHER PROCESS CONTROLS

Physical	**Technical**	**Procedural**	**Governance**
None	Knowledge of security threat environment and attack methods	• Metrics definitions • Forensic procedure	• Incident Analysis • Report

6. CYBERCECURITY REPORTING SYSTEM

The Securities and Exchange Commission ("SEC") has implemented regulations regarding cybersecurity disclosures for public companies. These regulations aim to enhance investor protection by ensuring transparency and awareness of potential cyber threats that could impact a company's financial health.

The SEC mandates public companies to disclose two main types of cybersecurity information:

1. **Material Cybersecurity Incidents:** Companies are required to disclose all **material** cybersecurity incidents they experience on **Form 8-K (Form 6-K for Genenta**) **<u>within 4 (four) business days of determining the materiality.</u>**

While the specific details may vary depending on the incident, a disclosure of a material cybersecurity incident on should generally address the following aspects:

- **Nature and Scope of the Incident:** This describes the type of cyberattack experienced (e.g., data breach, ransomware attack), the systems or data affected, and the estimated timeframe of the incident.
- **Timing of the Incident:** This specifies when the company became aware of the incident and the timeframe during which it potentially impacted the company's systems or data.
- **Material Impact:** This section explains the actual or potential material impact of the incident on the company's financial condition, operations, reputation, or legal compliance.
- **Remediation Efforts:** This describes the steps the company has taken or is taking to address the incident, mitigate any ongoing risks, and prevent similar incidents in the future.

2. **Cybersecurity Risk Management:** Companies are required to disclose annually, in their **Form 10-K** filings (**Form 20-F for Genenta**), information regarding their cybersecurity risk management strategies, policies, and procedures. This disclosure should provide investors with a general understanding of the company's approach to cybersecurity and its preparedness for potential cyberattacks.

6.1 Incident Management Process Table and Material Incident Reporting Time Table

Below is the timetable concerning the phases of the Incident Management process as described above, aimed at better understanding and identifying the main responsible parties for each phase, especially in case of material incident.

In case of a material incident, the CISO informs the Security Committee and the Security Committee notify notifies the Senior Management Team. Senior Management Team includes at least the Chief Executive Officer ("CEO"), the Chief Financial Officer ("CFO") and the Chief Medical Officer & Head of Development ("CMO").

An Action Plan that includes, where necessary, the Containment, Eradication, and Remediation activities should be drafted by the CISO, consulted with the Security Committee, and added to the Incident record.

Based on roles and responsibilities as defined by the RACI matrix presented under S**ection 4,** the Incident Management Process Table is the following:

PHASE	USER OR SYSTEM SOURCE	IT MANAGER	CISO	IT SECURITY COMMITTEE	SENIOR MANAGEMENT TEAM	DPO	BoD
DETECTION	Responsible - Notifier	Accountable for analysis and answer	Consulted Party	Informed	Informed	-	-
ASSESSMENT:							
5 Worst Case	-	Responsible -Operating	Accountable for analysis and answer	Consulted Party	Responsible - final decision maker	Consulted Party	Informed
4 Severe	-	Responsible -Operating	Accountable for analysis and answer	Consulted Party	Responsible - final decision maker	Consulted Party	Informed
3 Major	-	Responsible -Operating	Accountable for analysis and answer	Consulted Party	Responsible - final decision maker	Consulted Party	Informed
2 Moderate	-	Responsible -Operating	Accountable for analysis and answer	Consulted Party	Informed	Informed	-
1 Minor	-	Responsible -Operating	Accountable for analysis and answer	Informed	Informed	-	-
CONTAINMENT	-	Responsible -Operating	Accountable for analysis and answer	Consulted Party	Responsible - final decision maker	-	-
ERADICATION	-	Responsible -Operating	Accountable for analysis and answer	Consulted Party	Responsible - final decision maker	-	-
REMEDIATION	-	Responsible -Operating	Accountable for analysis and answer	Consulted Party	Responsible - final decision maker	-	Responsible - final decision maker
POST-INCIDENT REVIEW	-	Consulted Party	Responsible -Operating	Informed	Informed if material incident	Informed if material incident	Informed if material incident
REPORTING	-	-	Responsible -Operating	Consulted Party	Informed if material incident	-	Informed if material incident

6.2 Material Incident Reporting Time Table

To ensure compliance with the principle of timeliness, especially in the assessment, remediation, and reporting phases of **those incidents identified as material**, following is presented the Incident reporting timetable:

PHASE	DEAD LINE	RESPONSIBLE	REPORT TO Security Committee	REPORT TO Senior Management Team	REPORT TO BoD
DETECTION	**T=0**	**IT MANAGER**	**X**	**X**	**-**
ASSESSMENT	**T=4**	**CISO**	**X**	**X**	**-**
REMEDIATION	**T=6**	**CISO**	**X**	**X**	**X**
Form 6-K	**T=8**	**Senior Management Team**	**-**	**-**	**X**

7. REVIEW AND REVISIONS

This SOP will be reviewed periodically (at least every three (3) years) and updated if necessary.

8. REASON FOR CHANGE

Not applicable as this is the first version of this document.

9. PREIOUS HISTORY OF SOP

Not applicable as this is the first version of this document

10. ANNEX 1: CYBERSECURITY PLAN AND STRATEGY REPORTING

An annual cybersecurity report is presented to the Board of Directors (“BoD”) to demonstrate the effectiveness of the Company’s cybersecurity plan and strategy. This report takes the form of a questionnaire that systematically addresses all relevant aspects that are considered the framework pillars of the enterprise cybersecurity strategy. The questionnaire's responses serve as a comprehensive and structured way to communicate the cybersecurity efforts, ensuring that the BoD is well-informed about the security practices and the measures in place to protect the Company:

1. **Assessment and Risk Analysis:**
   - Have been identified and assessed the Company's digital assets and potential threats specific to the biotech industry?
2. **Regulatory Compliance:**
   - Is the Company in compliance with industry-specific regulations and standards, if applicable?
3. **Data Classification and Handling:**
   - Have been classified data based on sensitivity, and do exist procedures for secure data handling?
4. **Access Control:**
   - Are strong access controls, user authentication, and least privilege access in place?
5. **Employee Training and Awareness:**
   - Are employees trained in cybersecurity best practices, and do they know how to report incidents?
6. **Network Security:**
   - Have been implemented network security measures, including firewalls and intrusion detection systems?
7. **Endpoint Security:**
   - Are antivirus and anti-malware software installed on all endpoints?
8. **Data Backup and Recovery:**
   - Is critical data regularly backed up and securely stored offsite?
9. **Vendor and Supply Chain Security:**
   - Does the Company assess third-party vendor security practices?
10. **Incident Response and Recovery:**
    - Has the Company developed an incident response plan, and is there a clear reporting and management chain?
11. **Security Auditing and Monitoring:**
    - Is real-time monitoring in place, and are regular security audits conducted?

12. **Physical Security:**
    - Are physical access points secured, and is there a surveillance and alarm systems in place?
13. **Encryption:**
    - Is encryption used for sensitive data at rest and in transit?
14. **Documentation and Policy:**
    - Does the Company have cybersecurity policies and procedures accessible to all employees, and are they regularly reviewed and updated?
15. **Cyber Insurance:**
    - Has the Company considered any cyber insurance to mitigate the financial impact of a breach?
16. **Regular Testing:**
    - Are penetration testing and vulnerability assessments regularly conducted?
17. **Budget and Resources:**
    - Have been allocated budget and resources for ongoing cybersecurity efforts?
18. **Continuous Improvement:**
    - Are evolving threats and technologies considered and reviewed regularly?
19. **Communication and Reporting:**
    - Is there a clear communication channel for reporting security incidents, both internally and externally?
20. **Legal and Law Enforcement:**
    - Has the Company established contact with legal counsel and law enforcement agencies for guidance in case of a significant security breach?

11. ANNEX 2 – INCIDENT TYPE

	Incident Type	Description	Examples
External Attack	**Denial of service/DDoS**	Large amounts of requests, coming from a large number of distributed sources, are sent to a node in the network to exhaust system resources by denying the ability to provide a service.	- unusual reduction in network performance (when opening files or accessing websites/web applications);- unavailability of a website/web application;- inability to access the web;- huge and abnormal amount of requests directed to the same system;- drastic increase in the number of spam e-mails received ("mailbombing").
	Technical intrusion	Any type of event that allow unauthorized persons to access Company information and computer systems.	- sniffing;- insertion of a third party between two endpoints to intercept and modify the communication between them, without them being aware of it;- interception of information directed towards a system, followed by the sending of the same information, subject to modification, to the target system of the communication;- circumvention of controls, access checks and system pathways to obtain access or control of protected resources.
	Presence of malware	Any type of event that causes the installation, without the user's knowledge, of malicious software inside a computer, hindering the daily performance of activities that require the use of computer systems.	- virus;- worm;- trojan;- keylogger.
	Social Engineering/Phishing/Spear Phishing	A type of attack that, through the involuntary involvement of Company employees, allows access to the information and IT systems owned by the same.	- Malicious attachments in e-mails;- Malicious URLs in e-mails or social media;- Attack vectors via Microsoft Office (macros, etc.); - Social media messaging services.
	Ransomware	The attacker obtains ownership of Company files and/or devices by denying the real owner the possibility of accessing them. In exchange for the possibility of being able to return to using the locked assets, the attacker asks for a ransom in cryptocurrency.	- Screen locked with a ransom asking message.

	Incident Type	Description	Examples
	Web-based attack	A type of attack that uses web services as a means of compromising the Company's systems.	- Browser exploitation e browser injection;- Content Management System exploitation;- URL redirection attack;- Man in the browser attack.
	Data Breach	Compromise of security that results in the destruction, loss, alteration, unauthorized disclosure, or access to sensitive data transmitted, stored, or processed by Company.	- Data theft; - Inadvertent disclosure of data via email; - Loss of laptops, mobile devices, or USB sticks.
	Websites defacement	Any type of modification made by an external party to the Company's web pages, without the latter's knowledge.	- Changes in the appearance of websites (scribbled words/images, etc.).
	Third-party security incident (customer/service provider)	Any type of event related to security attacks perpetrated against the Company's customers or service providers that cause damage to the latter.	- Attacks on telecommunications services;- Theft of data stored in external infrastructures.
Anomalous internal behavior	**Elevation of privilege**	Any form of internal conduct aimed at the illegitimate acquisition of rights and privileges.	- users who use their rights outside the conditions provided for (misuse of administrator rights, etc.); - users who take possession of the rights of another employee; - Users who take over the identity of another employee.
	Resource used for illicit purposes	Type of event in which the resources made available are used for illicit purposes.	- presence of unauthorized software that may be used for malicious purposes; - use of resources for non-business purposes;- presence of reprehensible and criminal content (child pornography, etc.).
	Disclosure of information	Any form of event characterized by the unauthorized disclosure of information within the Company perimeter.	- disclosure by a Company employee of information to a colleague who is not authorized to access that type of information;- sharing of confidential information on the Company intranet.
	Other	An attack that does not fit into any of the other categories.	-

Effective Date: 2024/06/15

12. ANNEX 3 – CONTACT LIST

Role	Name Surname	Phone number	Mail
CISO	Mattia Campagner	+39 3402332175	Mattia.campagenr@bgt.it.gt.com
Finance Director	Barbara Regonini	+39 3386279028	barbara.regonini@genenta.com
IT Manager	Claudio Monastero	+39 3287286964	info@claudiomonastero.com