CYBER SECURITY POLICY

Genomma Lab.®
Internacional

OBJECTIVE

Our Cybersecurity Policy presents our guidelines and provisions to preserve the security of our technological infrastructure, data and systems. We are increasingly dependent on technology to collect, store and manage information and on third-party services, making us more vulnerable to serious security breaches. Human error, cyber attacks and system vulnerabilities could cause great financial damage and jeopardize our Company's reputation. For this reason, we have implemented a series of security measures. We have also prepared instructions that can help mitigate security risks. We have described both provisions in this Policy.

SCOPE

This Policy is applicable to all our employees, contractors and any person who has permanent or temporary access to all our systems, data and/or hardware.

1. DEFINITIONS

The terms below have the following meanings (all terms used in the singular in this document shall have the same meaning when used in the plural).

CONCEPT	MEANING/DEFINITION
Cyber Security	It is the set of practices, knowledge, people, reference frameworks, methodologies, tools and technologies included within various strategies that refer to the defensive position that the organization maintains in the face of a certain attack, event or security breaches, the above includes a prevention, detection and response program.
Confidentiality	Confidentiality refers to the ownership of information which implies that only authorized persons have access to and knowledge of said information. In the context of information security, confidentiality implies that sensitive or private data is protected from unauthorized access or disclosure.
Software	Program or set of computational instructions, as well as its associated data, procedures and guidelines that allow different tasks to be carried out in a computer system.
Antivirus	A type of software used to prevent, search for, detect, and remove viruses from a computer.
Clickbait	Writing technique that aims to get visits to a web page in order to increase advertising revenue.
Phishing	Technique to deceive users by exploiting their lack of caution and overconfidence to obtain personal information such as passwords, credit cards, bank accounts, etc. through a copy of the legitimate web page or through communications by email or messaging in which the identity of the original company is impersonated.
Malware	Any malicious program or code that intends to exploit vulnerabilities in systems for the purpose of causing damage and stealing confidential information.

2. CONFIDENTIAL INFORMATION

- **SENSITIVE DATA IS SECRET AND VALUABLE. SOME COMMON EXAMPLES ARE:**
  - ▪ Unpublished financial information.
  - ▪ Data from clients, partners, suppliers and other interest groups.
  - ▪ Patents, television commercials, dossiers, contracts, formulas or new technologies.
  - ▪ Customer lists (existing and prospective).
  - ▪ Corporate databases.

All our employees, partners, suppliers and contractors are obliged to protect this data and any other derivative of the original data. In this Policy, we present instructions for our employees on how to avoid security breaches. All information or digital element considered by Genomma Lab Internacional as confidential must be protected.

3. PROTECTION OF PERSONAL AND COMPANY DEVICES

When employees use their digital devices to access Company emails or accounts, they introduce a security risk to our data. We advise our employees to keep both their personal computers, tablets and cell phones and those of the Company safe. Recommendations for securing devices are as follows:

- Keep all devices password protected by changing it regularly.
- Verify that the assigned computers have the corporate antivirus.
- Make sure that you do not leave devices exposed, that is, without the necessary locks that allow anyone else to use the personal device.
- Check for availability of application, browser, and operating system updates monthly or as soon as updates are available that need to be installed.
- Reboot computers daily to ensure updates install properly.
- Log into Company accounts and systems only through secure and private networks.
- Report immediately to "Help Desk" (mesadeayuda@genommalab.com) any security incident, including temporary or permanent loss of equipment, as well as theft.

You should avoid accessing internal systems and accounts from other people's devices or lending your own devices to others.
In the event of having to access the Company's technological infrastructure or systems from other devices, all sessions must be closed and all information deleted.
If you do not have the two-factor authentication security feature for email, you must request it from the "Help Desk" (mesadeayuda@genommalab.com).
When a new employee receive equipment or electronic devices issued by the Company, they will receive instructions about:

- Appropriate use of passwords and compliance with password policies.
- Use of antivirus/antimalware software.
- Recommendations for the proper use of the devices.

They should follow the instructions to protect their devices and consult our "Help Desk" engineers (mesadeayuda@genommalab.com) if you have any concerns or questions.

4 . SECURITY FOR EMAILS

Emails often harbor scams and malicious software (for example, viruses). To prevent virus infection or data theft:

- Avoid opening attachments and clicking links when the content is not explained properly (for example, "watch this video, it's amazing").
- Be suspicious of clickbait titles (for example, offering prizes or tips).
- Check the email and names of people you receive messages from to make sure they are coming from legitimate accounts.
- Look for inconsistencies (for example, grammatical errors, capitalization, or an excessive number of exclamation points).

If a collaborator does not trust the origin of any email received and suspects that it is not safe, they can consult our "Help Desk" (mesadeayuda@genommalab.com). If there is a suspicion of having been the victim of an attack that compromises the security of the information, the email should be forwarded to the account: 911@genommalab.com

Notifications will be sent to the Company in cases where there is a Cybersecurity risk that must be disclosed and in the face of which extraordinary prevention measures must be taken.

5. CORRECT PASSWORD MANAGEMENT

Password leaks are dangerous as they can compromise our entire infrastructure. Passwords must not only be strong so they are not easily hacked, but they must also remain secret.
User accounts and passwords should NEVER be shared. Genomma Lab Internacional will consider these as serious crimes, which may result in the termination of the employment relationship and legal actions against the culprits.
For this reason, we advise our employees:

- Choose passwords with at least eight characters, (including upper and lower case letters, numbers, and symbols) and avoid information that can be easily guessed (for example, birthdays).
- Remember passwords instead of writing them down.If an employee needs to write their passwords, they are obliged to maintain the confidentiality of the paper or digital document and destroy it when they finish their work.
- Change your passwords according to the password policy of the different technological resources: networks, corporate systems (SAP, Dynamics, etc.).Remembering a large number of passwords can be tricky. The services of a password management tool will be used to securely generate and store passwords. In case of using the services of a password management tool, employees are obligated to create a secure password for the same tool, following the advice mentioned above.

6. SECURE DATA TRANSFER

- Avoid transferring sensitive data (for example, customer information or employee records) to other devices or accounts unless absolutely necessary. When the massive transfer of said data is required, we ask our employees to request help from "Help Desk" (mesadeayuda@genommalab.com).
- Share sensitive data over the Company's network/system and not over public Wi-Fi or private connection.
- Use for data transfer, only the technological resources that the company makes available for such purposes, ruling out the use of public services in the cloud (DropBox, WeTransfer, Google Drive, etc.).
- Make sure that the recipients of the data are duly authorized persons or organizations and have adequate security policies.
- Report scams, privacy violations and hack attempts.

Our "Help Desk" service (mesadeayuda@genommalab.com) requires knowledge about scams, breaches, and malware in order to best protect our infrastructure. For this reason, we advise our partners to report perceived attacks, suspicious emails or phishing attempts to our specialists as soon as possible.
Our IT Engineers must promptly investigate, resolve the issue and alert the entire company when necessary. Our Security Specialists are responsible for advising employees on how to detect fraudulent emails. We encourage our employees to contact them with any questions or concerns.

7. ADDITIONAL MEASURES

To reduce the likelihood of security breaches the following should be considered:

- The Company's executive staff and leaders must be responsible and collaborate in the dissemination and adoption of the Cybersecurity Policy.
- All our employees must consult the resources (courses, manuals, documentation) provided by the IT area for training.
- Turn off their screens and lock devices when not in use. Provide the necessary seriousness and time when employees are required by the Help Desk and/or IT staff to address incidents, breaches or vulnerabilities.
- Report stolen or damaged equipment as soon as possible to Human Resources, IT and Legal departments.
- Change all account passwords immediately when a device is stolen.
- Report any perceived threat or potential security weakness in Company systems.
- Refrain from downloading or installing unauthorized software on Company equipment.
- Avoid accessing suspicious websites, gaming and betting sites, adult content, etc.
- Avoid using public messaging applications, social networks or personal emails to share Company information. For example. When using WhatsApp, even if the data is encrypted, it is available to other companies (Facebook/Meta).

8 . RESPONSIBILITIES OF THE IT DEPARTMENT

- Install firewalls, anti-malware software and access authentication systems.
- Manage safety training for all employees.
- Inform employees regularly about new emails or scam viruses and ways to combat them.
- Investigate security breaches thoroughly.
- Follow the provisions of this Policy as other employees do.
- Generate daily reports with statistics on incoming email from external domains with suspicious activity.
- Be informed by the Human Resources department about the hiring and firing of employees to take the appropriate measures regarding the availability of accounts and electronic equipment, etc. Our Company will have all the physical and digital shields to protect the information.

Remote employees must follow the instructions of this Policy without exception. Since they will be accessing Company accounts and systems from a distance, they are also required to follow all data encryption, protection standards and settings, and ensure that their private network is secure. Employees must be connected through VPN and/or through any other encryption method, also through password policies implemented by the IT Department. We encourage you to seek advice from our Security Specialists and IT Administrators.

9. WORK AT HOME AND REMOTE WORK

Remote employees must follow the instructions of this Policy without exception. Since they will be accessing Company accounts and systems from a distance, they are also required to follow all data encryption, protection standards and settings, and ensure that their private network is secure. Employees must be connected through VPN and/or through any other encryption method, also through password policies implemented by the IT Department. We encourage you to seek advice from our Security Specialists and IT Administrators.

10. DISCIPLINARY ACTIONS

We expect all our employees to follow this Policy. Those who cause security breaches may face disciplinary action:

- Small-Scale, Unintentional, First-Time Security Breach: A verbal warning may be issued and employee may be trained on security issues.
- Intentional, repeated or large-scale violations (causing financial or other serious damage): We will invoke more severe disciplinary measures up to and including termination of employment.

- We will examine each incident on a case-by-case basis. Additionally, employees/associates who fail to adhere to security instructions will face progressive discipline, even if their behavior has not resulted in a security breach.

Genomma Lab Internacional team, from our clients and partners to our employees and contractors, must feel that their data is safe. The only way to earn your trust is to proactively protect our systems and databases. We can all contribute to this by being vigilant and keeping cybersecurity in our minds everyday.

Marco Sparvieri
CEO
July, 2023