Cybersecurity Global Policy

Genomma Lab.® International

Purpose

Our **Cybersecurity Policy** outlines our guidelines and provisions for **preserving the security of data and technology infrastructure.**

The more we depend on technology to collect, store and manage information, the more vulnerable we become to suffer severe security breaches. Human errors, hacker attacks and system malfunctions could cause great financial damage and may jeopardize our Company's reputation.

For this reason, we have implemented a **number of security measures**. We have also prepared instructions that may **help mitigate security risks**. We have outlined both provisions in this Policy.

Scope

This policy **applies to all our employees, contractors and anyone** who has **permanent or temporary access to our systems and/or hardware**.

Policy

Confidential data

Confidential data is secret and valuable. Common examples are:

- Unpublished financial information
- Data of customers, partners, vendors and other stakeholders
- Patents, TV ads, dossiers, contracts, formulas or new technologies
- Customer lists (existing and prospective)
- Corporate Data bases

All employees, partners, vendors and contractors are obliged to protect this data and any other derived from the original data. In this Policy, we present instructions for our employees on how to avoid security violations.

Every information or digital element considered by Genomma Lab as a confidential must be protected.

When employees use their digital devices to access Company emails or accounts, they introduce security risk to our data. **We advise our employees to keep both their personal and Company-issued computer, tablet and cell phone secure**. To make sure of this:

- Keep all devices **password protected by changing them on regular basis**.
- Choose and **upgrade a complete antivirus software**.
- **Make sure not to leave the devices exposed or unattended**.
- **Install security updates of browsers and operating systems monthly** or as soon as updates are available.
- **Log into Company accounts** and systems through **secure and private networks only**.

We also advise our employees to avoid accessing internal systems and accounts from other people's devices or lending their own devices to others.

When new hires receive Company-issued equipment or electronic devices they will receive instructions for:

- Appropriated use of passwords and compliance to password policies
- Use of antivirus/anti-malware software

They should **follow instructions** to protect their devices and refer to our ***"Mesa de Ayuda"*** Engineers (mesadeayuda@genommalab.com) if they have any questions.

Keep emails safe

Emails often host frauds and malicious software (e.g. virus). To avoid virus infection or data theft, we instruct employees to:

- **Avoid opening attachments and clicking on links** when the content is not adequately explained **(e.g. "watch this video, it's amazing.").**

- **Be suspicious of clickbait titles** (e.g. offering prizes or advice).

- **Check email and names of people they received a message** from to ensure they are legitimate.

- **Look for inconsistencies** (e.g. grammar mistakes, capital letters, excessive number of exclamation marks).

If an employee isn't sure that an email he received is safe, he can refer to our *"Mesa de Ayuda"* (mesadeayuda@genommalab.com).

Regular communication will be shared to the Company regarding anti-phishing and malware, giving advice and security instructions regarding suspicious messages.

Manage passwords properly

Password leaks are dangerous since they can compromise our entire infrastructure. Not only should passwords be secure so they won't be easily hacked, but they should also remain secret.

User accounts and Passwords are NEVER meant to be shared. Genomma Lab will consider these as grave offenses, which may result in the termination of labor relations and legal actions against offenders.

For this reason, we advice our employees to:

- **Choose passwords with at least eight characters,** (including capital and lower-case letters, numbers and symbols) and avoid information that can be easily guessed (e.g. birthdays).

- **Remember passwords instead of writing them down**. If employees need to write their passwords, they are obliged to keep the paper or digital document confidential and destroy it when their work is done.

- **Change your passwords every two months**. Remembering a large number of passwords can be difficult. The services of a password management tool will be used to safely generate and store passwords. Employees are obliged to create a secure password for the tool itself, following the abovementioned advice.

Transfer data securely

Transferring data introduces security risk. To prevent it:

- **Avoid transferring sensitive data** (e.g. customer information or employee records) to other devices or accounts unless it is absolutely necessary. When mass transfer of such data is needed, we request employees to ask our *"Mesa de Ayuda"* (mesadeayuda@genommalab.com) for help.

- **Share confidential data over the Company network/ system and not over public Wi-Fi or private connection**.

- **Ensure that the recipients of the data are properly authorized people or organizations and have adequate security policies**.

- Report scams, privacy breaches and hacking attempts.

Our ***"Mesa de Ayuda"*** (mesadeayuda@genommalab.com) **need to know about scams, breaches and malware so they can better protect our infrastructure**. For this reason, we advise our employees to report perceived attacks, suspicious emails or phishing attempts as soon as possible to our specialists. Our *IT Engineers* must investigate promptly, resolve the issue and send a companywide alert when necessary.

Our Security Specialists are responsible for advising employees on how to detect scam emails. We encourage our employees to reach out to them with any questions or concerns.

Additional measures

To reduce the likelihood of security breaches, we also instruct our employees to:

- Turn off your screens and lock your devices when leaving your working places.
- Report stolen or damaged equipment as soon as possible to HR, *IT and Legal Departments*.
- Change all account passwords at once when a device is stolen.
- Report a perceived threat or possible security weakness in Company systems.
- Refrain from downloading suspicious, unauthorized or illegal software on their Company equipment.
- Avoid accessing gambling websites, responsible use of the internet and social media.

Our IT department should

- Install firewalls, antimalware software and access authentication systems.
- Arrange for security training to all employees.
- Inform employees regularly about new scam emails or viruses and ways to combat them.
- Investigate security breaches thoroughly.
- Follow this policies provisions as other employees do.
- Generate daily reports with statistics about incoming email from external domains with suspicious activity.
- Be informed by the Human Resources department about hiring and employees terminations in order to take the appropriate measures about accounts and equipment availability, etc.

Our Company will have all physical and digital shields to protect information.

Home office and remote work

Remote employees must follow this Policy's instructions too. Since they will be accessing our Company's accounts and systems from a distance, they are obliged in addition, to follow all data encryption, protection standards and settings, and ensure their private network is secure.

Employees will have to be connected thru VPN and/or using any other encryption methods, also using password policies implemented by IT Department.

We encourage them to **seek advice** from our Security Specialists and IT Administrators.

Disciplinary action

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

- First-time, unintentional, small-scale security breach: We may issue a verbal warning and train the employee on security issues.
- Intentional, repeated or large scale breaches (which cause severe financial or other damage): We will invoke more severe disciplinary action up to and including termination of the labor relationship.
- We will examine each incident on a case-by-case basis. Additionally, employees who are observed to disregard the security instructions will face progressive discipline, even if their behavior has not resulted in a security breach.

Take security seriously

All the Genomma Lab team, from our customers and partners to our employees and contractors, should feel that their data is safe. The only way to gain their trust is to proactively protect our systems and databases. We can all contribute to this by being vigilant and keeping cybersecurity top of mind at all times.

Jorge Luis Brake Valderrama
CEO
June, 2020