

Blue Pepper B.V.
Information Security Policy
Version 1.0

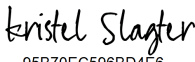
Document Information

Subject	Information Security Policy
Purpose	To set out the policy stance on Information Security
Document Owner	Head of IT
Review	Annually or as early as required
Involvements	All departments.
Approval	Executive management
Document Classification	Internal Use.

Version Control

Date	Version	Title	Description
03/06/2025	1.0	Head of IT	Document creation

Approval

Date	Version	Title	Signature
6/5/2025	1.0	Director	DocuSigned by:  95B70EC596BD4E6...

1. Scope

This policy applies to:

- board members
- all staff, including managers and supervisors; full-time, part-time or casual, temporary or permanent staff; job candidates; apprentices, contractors, subcontractors and volunteers
- how Blue Pepper B.V. (referred to as - BP) provides services to clients and how it interacts with other members of the public
- all aspects of employment, recruitment and selection; conditions and benefits; training and promotion; task allocation; shifts; hours; leave arrangements; workload; equipment and transport
- on-site, off-site or after-hours work; work-related social functions; conferences – wherever and whenever staff may be as a result of their BP duties
- staff treatment of other staff, clients, and other members of the public encountered in the course of their work duties.

2. Aims

This policy outlines our guidelines and provisions for preserving the security of our data and technology infrastructure.

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

Everyone, 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 cyber security top of mind.

3. Policy Elements

3.1 Confidential Data

Confidential data is secret and valuable. Common examples are:

- Unpublished financial information
- Personal data of customers/employees/partners/vendors
- Intellectual property, including, patents, formulas, or new technologies

- Customer lists (existing and prospective)

All employees are obliged to protect this data. In this policy, we will give our employees instructions on how to avoid security breaches.

3.2 Protect personal and company devices

When employees use their personal digital devices to access company emails or accounts, they introduce security risks to our data. Use of personal devices for work must be approved by the employee's manager.

We advise our employees to keep both their personal and company-issued computer, tablet, and cell phone secure. They can do this if they:

- Keep all devices password protected.
- Choose and upgrade a complete antivirus software.
- Ensure they do not leave their devices exposed or unattended.
- Install security updates of browsers and systems monthly or as soon as updates are available.
- Log into company accounts and systems through secure and private networks only.

Employees must 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 they will receive instructions for security and password management tool setup. Anti-virus and anti-malware software is pre-installed on the device.

They should follow instructions to protect their devices and refer to our IT Department if they have any questions.

3.3 Keep emails safe

Emails often contain scams and malicious software (e.g. viruses, worms.) To avoid virus infection or data theft, we instruct employees to:

- Avoid emails that are unexpected, request sensitive information (e.g., username, passwords), contain suspicious links or attachments, or use urgent or threatening language.
- Be suspicious of clickbait titles (e.g. offering prizes, advice.)
- Check email and names of people they received a message from to ensure they are legitimate.

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

If an employee isn't sure that an email they received is safe, they can refer to our IT Department.

3.4 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. For this reason, we advise 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.
- Exchange credentials only when absolutely necessary. When exchanging them in-person isn't possible, employees should prefer the phone instead of email, and only if they personally recognize the person they are talking to.
- Change their passwords every two months.

Remembering many passwords can be daunting. The Company uses password management tools which generate and store strong passwords. Employees must create a secure password for the tool itself, following the above-mentioned advice.

3.5 Transfer data securely

Transferring data introduces security risk. Employees must:

- Avoid transferring sensitive data (e.g. customer information, employee records) to other devices or accounts unless absolutely necessary. When mass transfer of such data is needed, we request employees to ask our IT Department for help.

- All data sent over email (as an attachment or in an email text) should be considered sensitive and protected as such. Never send work documents or information to someone outside of the company unless it has been cleared by a manager and IT. *This includes forwarding company emails to your own personal email.*
- Sharing of data through chat system like Team, Skype, WhatsApp, should be avoided. In exceptional cases, data may be sent if encrypted, with the password shared separately via another channel, like SMS.
- Avoid transferring of data to external devices such as disks, USB sticks, CD, DVD.
- Share confidential data over the company network/system and not over public Wi-Fi. If not possible, personal mobile hotspot should be used.
- 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.

Employees should promptly report any suspicious emails, phishing attempts, or potential security threats or data breaches to the IT Department or the Data Protection Officer (DPO). This helps ensure timely investigation, resolution, and, when needed, a companywide alert to protect our systems.

Our IT Department is responsible for advising employees on how to detect scam emails. We encourage our employees to reach out to the IT Department with any questions or concerns.

3.6 Additional measures

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

- lock their devices when leaving their desks.
- Report stolen or damaged equipment as soon as possible to HR or IT team.
- Change all account passwords immediately when a device is stolen.
- Report a perceived threat or possible security weakness in company systems.
- Refrain from downloading suspicious, unauthorised or illegal software on their company equipment.
- Avoid accessing suspicious websites.

Our IT Department should:

- Install firewalls, anti-malware 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.

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

3.7 Remote employees

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 to follow all data encryption, protection standards and settings, and ensure their private network is secure.

They should contact the IT Department if they have any security concerns or need technical support.

4. Violations of the Policy

If an employee violates this policy, he or she may be subject to termination or other disciplinary action to prevent future violations. The following individuals may be subject to disciplinary action or termination:

- Employees who are in direct violation of this policy.
- Employees who deliberately withhold information concerning the violation of this policy or fail to report a violation of this policy.
- Management personnel who fail to report violation of this policy by their subordinates.

5. Other relevant policies

Staff, especially managers and supervisors, are encouraged to read this policy in conjunction with other relevant BP policies, including:

- [Data Protection Policy](#)
- [Data Breach Response Policy](#)

6. More information

If you have a query about this policy or need more information, please contact the IT department.