Introduction

This declaration aims to provide ING joiners with guidelines on information security. At the end of the document, there is a section which the joiner will need to sign to indicate his/her acceptance to observe and adhere to these guidelines.

Information and all IT systems that support your work are critical business assets of ING for profitability and respected company image. The role of each employee, contractor, third party or vendor is to protect these assets, to prevent unauthorized disclosure and to ensure the accuracy and completeness of the information we all depend upon for business continuity.

This declaration composed of the Information Risk Management (IRM) Security Guideline and relevant ING Group policies and standards and the Code of Conduct.

Employment at ING

As a condition of employment at ING, you will be bound by the confidentiality clause in your employment contract and diligently protect all ING's systems, information, and data from unauthorized disclosure. All users of ING's information systems are required to comply with the security policies. Non-compliance can result in disciplinary actions, revocation of systems privileges and includes up to termination of employment or service agreements, civil or criminal liability and/or recovery of damages.

During your employment:

- ING has legal ownership of the contents of all files stored on its computer and network systems as well as all messages transmitted via these systems. ING reserves the right to access this information without prior notice whenever there is a genuine business need.
- ING does not engage in blanket monitoring of employee communications. It does, however, reserve the right to monitor, access, retrieve, read and/or disclose employee communications.
- Employees and systems users are encouraged not to store personal files on ING computers and removable disks. If employees choose to store such personal files, these files are treated as the property of ING.
- Employees are not allowed to send documents with ING data to personal e-mail address and drivers.
- ING has the right to:
  - Monitor all access and use of its resources, facilities and authority relating to the public Internet and e-mail.
  - Make information it obtains through such monitoring or otherwise, available internally and/or externally as deemed appropriate or necessary by ING management.

Workstation Security

ING operates a 'clean desk' policy, which means that your work area should not have any sensitive or confidential information on display or easily accessible when unattended. This data can be either

Joiner Initial (Ex. Juan Ramos Dela Cruz = JRDC) :

paper or electronic format.

Joiner Initial (Ex. Juan Ramos Dela Cruz = JRDC) :

- Confidential or sensitive data should be cleared from your work area and placed in a secure environment when unattended. Use lockable pedestals, cabinets and lockers provided.
- All confidential documents that are no longer required should be disposed of using secure metal bins for shredding by 3rd party provider.
- Ensure all information has been removed from facsimile machines and printers after use.
- Lock your workstation before leaving your desk unattended for an extended period. (Shortcut: Press window icon + L.
- Log out of all systems and accounts at the end of each day to enable not only system updates but to ensure your PC's performance remains at its best.
- Any confidential or sensitive information contained on removable storage media (USB thumb drives, CDs, DVDs and portable hard drives) should be stored in a secure environment when not in use.
- Do not install freeware/unlicensed software on your desktop.

Password Security

Choose and treat your password very carefully. If someone has access to your password, they will have the opportunity to misuse the authorizations granted to you. You are responsible for actions taken with your systems accounts, and you should ensure that you are the **only one** who has knowledge of how to access them. If you think your password has been compromised or if you have any password queries, contact your Help Desk.

It should be noted that any user access or account misuse will be subjected to penalties as mandated by ING User Access Minimum Standard.

E-Mail Usage Guidelines

E-mail messages are the property of ING, regardless of their physical location, including, but not limited to ING premises and user residences. E-mail resource is for business use only and you should be aware when sending correspondence that a company disclaimer accompanies all outgoing messages. The company's reputation is at risk each time this facility is used incorrectly or abused.

Refer to guidelines for using communication channels that were released by CORM on 27th March 2023

Internet Usage Guidelines

With a connection to the Internet, an attacker could gain unauthorized access to internal ING network or introduce computer virus. Use the internet for business purposes only during contractual working hours and ING cautions users that this company resource is not to be misused.

Joiner Initial (Ex. Juan Ramos Dela Cruz = JRDC) :

Guideline:

- Do not use for unauthorized downloads or distribution of third-party software. If this is required for business purposes, contact your Help Desk to obtain the correct procedure.
- Internet usage should only be used for ING Hubs PH work-related items/instances.
- If you have a password on an Internet site, make sure it is not the same as your systems passwords.
- Do not disclose or make available or accessible ING company information, including any data that is confidential, proprietary sensitive or a trade secret.
- Close all active internet browsers before leaving your workstation.
- Copying programs and data is allowed only in connection with the execution of your professional tasks, after explicit approval from your superior and if ING is authorized to do so.
- Users shall not upload third party licensed software or software which has been developed by ING to any other computer via the Internet
- All ING users shall respect all laws surrounding copyrights, patents, trademarks, and the like when extracting information or material from the Internet.
- The following are examples of inappropriate internet usage and should not be practiced at all times:
  - Gain unauthorized access or compromise the security of any computer system
  - Viewing, receiving, sending, or storing of pornographic, indecent or any other offensive or immoral material
  - Make defamatory or derogatory remarks against ING as his/her employer in any social networking site
  - Hate speech and flaming
  - Propaganda

Instant Messaging Guidelines

Information exchanged during the use of IM systems is the property of ING, regardless of their physical location, including, but not limited to ING premises and user residences. Instant messaging resource is for business use only and you should be aware when sending information or correspondence that a company disclaimer accompanies all outgoing messages. The company's reputation is at risk each time this facility is used incorrectly or abused.

ING has the right to:

- Monitor all access and use of its resources, facilities and authority relating to the public Internet and e-mail.
- Make information it obtains through such monitoring or otherwise, available internally and/or externally as deemed appropriate or necessary by ING management.
- Take any action permitted by law, equity, or contract regardless of whether same results in civil or criminal proceedings against any person, firm or enterprise found or suspected of being in violation of this or related policies.

Joiner Initial (Ex. Juan Ramos Dela Cruz = JRDC) :

The use of Instant Messaging shall be centrally logged and all communications (i.e. IM chats and messages) will be monitored daily and recorded to secure effective system operation and for other lawful purposes. It is noted that the use of the IM system should only be for business purposes. Private use of the IM system may result in revocation of rights. Unauthorized and incorrect use of the IM systems will be reported to business management and can lead to disciplinary action up to and including dismissal as per current HR procedures and, in extreme case prosecution, or in the case of non-ING employees, termination of service agreements.

Guideline:

- The Instant Messaging communications should not be used to confirm trades or business dealings.
- All communications are to be treated as confidential and the information in it may not be used or disclosed except for the purpose for discussion. If a transaction is entered, its terms will be found entirely in the final documentation for the transaction and this communication may not be used to construe such terms.
- Employees of ING are required not to make any defamatory statements and not to infringe or authorize any infringement of copyright or any other legal right in any communications made by them.
- ING will not accept any liability in respect of such a communication, and the employee responsible will be personally liable for any damages or other liability arising.
- Report any suspicions you may have immediately to the Help Desk.

Laptop Security

ING's laptops are important business assets, and their use is essential in maintaining our competitive edge. To ensure that this resource is used efficiently and securely, the following guidelines have been set and should be followed to sustain general laptop security.

Guideline:

- Keep your laptop always secured – lock it away when not in use.
- ING laptops shall be used for business activities ONLY.
- Take care when using laptops in public places, don't leave them unattended.
- All software and hardware used on the portable computers shall be approved and authorized by the ING management and the owner shall do everything possible to protect the assigned equipment and the data stored on such equipment.
- Preventative security measures shall be taken by ING personnel to prevent the theft and to protect sensitive/confidential information stored on the company portable computer.
- ING laptops are pre-configured with disk encryption software. Contact the Help Desk if in doubt.
- Back up your data regularly on network drives.
- Contact you Help Desk for regular virus software updates.
- When travelling, laptops should be carried as hand luggage and not checked in as baggage.

Joiner Initial (Ex. Juan Ramos Dela Cruz = JRDC) :

- Remote access to corporate emails and other ING applications should be applied through normal procedure with Help Desk.
- Any information that helps an unauthorized user in gaining access to a laptop needs to be kept separate from the machine. Examples of such instances include notes with passwords, ING business cards and diaries.

Refer to ING Portable Computer Usage and Control Policy.

RSA SecurID Token

You may be assigned a RSA SecurID Token to perform second factor authentication to your laptop or for remote access to the ING Network or Webmail. This system creates an audit trail that cannot be repudiated, you may be held accountable for activities recorded identifying you as the perpetrator.

You are responsible for protecting the authentication factors entrusted to you. Keep your PIN secret and protect your SecurID token against loss and theft.

If an unauthorized person learns your PIN and obtains your token, this person can assume your identity. Any action this intruder takes is attributed to you in the system's security log.

For your own protection and that of the system, always take the following precautions:

- Never reveal your PIN or user password to anyone. Do not write them down.
- If you think someone has learned your PIN, notify the security administrator, who will clear the PIN immediately. At your next login you will have to receive or create a new PIN.
- Exercise care not to lose your RSA SecurID token or to allow it to be stolen. If your token is missing, inform your IT Helpdesk immediately. The administrator will disable the token so that it is useless to unauthorized users, or assign you a temporary password.
- Do not let anyone access the system under your identity (that is, log in with your PIN and a token code from your SecurID token).

Computer Virus Information

Computer viruses can irreparably disrupt and destroy programs and data. Viruses can replicate, disable, and damage systems. Some remain dormant only to activate at a later date. The resulting cost of a virus attack can range from resource time and effort to repair, to the loss of data, and therefore business and reputation. Viruses do not only spread to PCs and networks by disks, but they can also be introduced via e-mail, Internet downloads and third-party software.

Guideline:

- Do not download unauthorized software from the Internet.
- Ensure all third-party software has been thoroughly checked before installation. Contact your Help Desk for procedure.

Joiner Initial (Ex. Juan Ramos Dela Cruz = JRDC) :

- Do not open e-mails from unknown sources.
- Do not directly open files attached to your e-mail messages, choose the 'file, save' option available which will scan for possible viruses.
- Ensure your laptop or PC has the latest system patches, virus updates and all other applications updates.

Lost or Stolen Information Assets

For confidential lost or stolen information, data, software or any other Information Technology resource (such as Blackberry, laptops, SecurID tokens, DISA codes, PDA, USB drive with restricted data), or suspected of being so, notify your manager and the Operational Risk Management or IT department **immediately**.

Any other information asset (ID badges, access cards, business-issued credit cards or mobile phones) that has been suspected of being lost or stolen should be reported to the issuing department as soon as noticed. An incident report should also be raised.

Refer to your locally approved Lost Assets Policy for fines on lost assets. If you have queries regarding the policy, contact your immediate supervisor.

Use of Mobile Devices

All users of ING mobile devices are required to comply with this policy. Non-compliance can result in disciplinary action, up to and including termination of employment. ING intends to honour this policy and reserves the right to change it at any time. When changes are made, the revised Policy shall be available to all users at the ING Intranet site.

- All ING personnel shall keep their passwords secret and shall be held responsible for the safekeeping of information and taking preventive steps to avoid unauthorized disclosure.
- Confidential computer data shall be protected using CISO approved encryption mechanism and logical access controls installed on the portable computers hard drive.
- In case a group or a location is sharing a pool of portable computers, one of these users shall be formally appointed as the owner. Such owner shall also be responsible for assigning, keeping track, and collecting such portable computers from the users.
- Mobile devices shall always be locked away in a safe place when not in use in the office or at remote locations.
- Any information that helps an unauthorized user in gaining access to a laptop needs to be kept separate from the machine. Examples of such instances include notes with passwords, ING business cards and diaries.

Joiner Initial (Ex. Juan Ramos Dela Cruz = JRDC) :

Policies and Standards

If you wish to learn more about your responsibilities and accountability towards information and IT systems belonging to ING, we recommend that you read the Information (Technology) Risk Policy and the User Access Minimum Standard.

The full list can be found at the Global ORM (Information Technology Risk) Portal

By signing below, I accept these guidelines and agree to abide by them during my employment with ING.

	Joselito Buenaventura	September 1, 2025
Signature	Print Name	Date

Retail Tech - Belgium 7

Department / Division