Rabobank

Responsible Use Policy for IT systems - EU Region

Information Security Europe

FINAL- Version 0.3 – December 2017

Document control information

Version control

Date	Version	Author	Reviewers	Summary of changes
15/09/2015	0.1	Theo Walraven		Initial Draft
27/09/2015	0.2	Theo Walraven		2nd draft
23/10/2017	0.3	Mark Jacob	RCSE	Update for interim use pending GISO policy update

Approvals

This document requires the following approvals.

Title	Name	Approval date
RSCE	Regional Security Committee Europe	11th December 2017

Document owner

The Head of Security Europe is the owner of the document and can be contacted for questions or suggestions.

Distribution

Title	Name	Date
Security Europe		
RSCE members		
Branch contacts Security		
HR Europe		

Publication

Name	Title	Date

Table of contents

1 Introduction

The IT systems and the information they contain are valuable assets of Rabobank. If the availability, integrity or confidentiality of our information systems cannot be guaranteed, this can result in significant direct or indirect financial and/or reputational risk to the Bank.

Users need to know how they can securely and responsibly use the IT systems in order to protect Rabobank against ever growing security threats. Rabobank takes various measures to ensure this protection of information as well as that of their employees.

This document defines the responsible use (of IT) policy within the branches of Rabobank within the WRR EU Region.

This document has been made as *TEMPLATE* that can be used 'as is' or be amended to the local branch situation, if required.

1.1 Objectives

The purpose of this document is to articulate the policy of the Bank in protecting its IT systems and their information. The objectives are to:

- Protect the Bank's IT systems and their information against internal and external security threats
- Protect the Bank's assets and reputation as a financial institution and as an employer;
- Inform the users of their duties and rights and provide guidelines;
- Inform the users of the Bank's rights.

1.2 Scope

This policy applies to all forms of IT systems provided by the Bank, including, but not limited to: desktop PCs, laptops, smart phones, tablets, all forms of removable media, and all associated information, data and applications. It also applies to privately owned devices that are approved for using for Rabobank business purposes.

The policy is applicable to all permanent and temporary employees, agency staff and consultants/ contractors who are provided with access to any of Rabobank IT systems.

1.3 Related documents

Related topics are described in the following documents:

1. **Information Handling and Information barriers** document(s) from Compliance
2. **Data Privacy Policy** document(s) from Privacy Officer (/ General Data Protection Regulation)

2 Duties and rights of Users

2.1 Duty to Comply

IT systems provided by the Bank must be used at all times in a responsible, professional, lawful and ethical manner, in compliance with this policy.

In addition, users are responsible for complying with copyright law and applicable licenses that may apply to software, files, graphics, documents, messages, and other material they wish to download or copy.

Security settings and protection measure may not be switched-off, changed or by-passed. Existing procedures must be followed and prescribed security measures must be used. Software that can influence the stability or security in the workplace may only be installed by authorised IT system administrators.

2.2 Duty to Protect

Users are responsible for protecting the information and resources required by the Bank in the conduct of its business.

Users are responsible for protecting the Bank's reputation as a financial institution and as an employer. In particular, all files and email messages obtained from any sources outside the Bank may contain dangerous computer viruses or links to phishing websites.

All email messages sent to external recipients from the Bank computer systems must be sent with an approved disclaimer. (This is normally applied automatically by our regional mail gateways but it is worth checking that it meets local requirements)

The Bank absolutely prohibits all users (unless expressly authorised to do so) from sending, transmitting, or otherwise distributing to external parties, proprietary information, data, trade secrets or other confidential information belonging to The Bank, or belonging to its customers or clients or in respect of which the Bank is subject to a confidentiality obligation.

2.3 Duty to Report (Security Incident Handling)

Users are responsible for the immediate reporting of all suspected security incidents to their Line Manager or Local/Regional Security officer.

All reported incidents will be dealt with in confidence, and the associated information will be handled at all times in accordance with all applicable local privacy laws and prevailing data protection regulations.

Incidents escalation will follow the global 'Security Incident Handling Process' and/or specific local procedure if such exists.

2.4 Duty to Co-operate

Users must co-operate with all security investigations.

2.5 Handling confidential information

IT systems may contain confidential information and this information needs to be handled in line with Rabobank Data privacy policies and local regulations that apply.

3 Duties and Rights of the Bank

The Bank regards all electronic data and communications to, from, and stored in, its computer systems as the property of the Bank.

3.1 Right to Protect

The Bank has the right to implement all appropriate measures to ensure that the computers and networks that are the property of the Bank are used in accordance with this policy.

The Bank has the right to block or quarantine certain types of email file attachments, which the Bank deems unsafe or inappropriate in the workplace.

The Bank has the right to utilise software that makes it possible to identify and block access to Internet sites containing offensive or pornographic material, or any other material the Bank deems unsafe or inappropriate in the workplace. The Bank has the right to utilise software that makes it possible to identify and block access to Internet services, which the Bank deems unsafe or inappropriate in the workplace.

3.2 Right to monitor

The Bank has the right to check and monitor if the computers and networks that are the property of the Bank are used in accordance with this policy. Based on this right the Bank continues to check and monitor the computers and networks that are the property of the Bank.

Where a security incident as defined in section 2.3 above, has been reported, the bank may without notice to users access the contents of files or email messages or any electronic information stored on the bank’s systems.

The investigation of security incidents will be undertaken only by authorised officials. The information gained during this exercise will be treated in the strictest confidence.

3.3 Right to Log and Review

The Bank has the right to log and review any and all aspects of its IT systems including, but not limited to, system access times, monitoring Internet sites visited by users and monitoring file downloads. Based on this right the Bank continues to log and review all aspects of its computer systems.

This logging and reviewing will only be undertaken by authorised IT or Security staff to protect the bank against irresponsible internal usage and external threats.

3.4 Right to Access

Access to monitoring data and access to any other data repositories which may contain personal information will be restricted to authorised staff for limited periods of time, and handled at all times in accordance with all applicable privacy laws and prevailing data protection regulations.

4 Specific guidelines

4.1 General Use

- The Bank absolutely prohibits users from revealing their passwords to anyone. Passwords must be changed periodically and must be difficult to guess. Passwords must never be written down.

- The Bank absolutely prohibits attempts to gain access to resources or any account on any computer system to which you are not explicitly authorised.

- The Bank absolutely prohibits the sharing and usage of accounts or communication tools where a user's identity could be misrepresented or unclear.

- Without prior written permission from the Local Management, the Bank absolutely prohibits the use of its computer equipment to join any external service where the name of the Bank could be misrepresented.

- The Bank absolutely prohibits the use of its computer resources to disseminate destructive code (e.g., viruses, Trojan horse programs, etc.), mail "bombs", "chain letters", and denial of service (DDoS) attacks or any other form of anti-social code or behaviour. If a user suspects that a virus has been introduced into the Bank's network, the user must notify the IT Service Desk immediately.

- Without prior written permission from the Local management, the Bank's computer network may not be used to purposely disseminate, view, forward, download or store advertisements, solicitations, promotions, or any other material for commercial or personal use other than in connection with The Bank business.

- The bank absolutely prohibits users from copying bank sensitive commercial or personal data to insecure external portable devices (such as non-Rabobank laptops, CD/DVD, USB memory sticks etc.) [For advice on how to appropriately transfer sensitive data please speak to your local IT support department or Local/Regional Security Officer]

- The Bank absolutely prohibits the connection of security compromised devices (e.g. "Jailbroken" or "rooted" iPhones/Android devices) to a Bank computer or its network as this may increase the chances of malware or viruses.

- Users must not deliberately perform acts that waste computer resources or monopolize resources to the exclusion of others. These activities include, but are not limited to:
  - Sending mass mailings and chain letters;
  - Spending excessive amounts of time on the Internet for personal reasons;
  - Playing computer games;
  - Engaging in online personal chat groups;
  - Uploading or downloading large files for personal use;
  - Otherwise creating unnecessary loads on network traffic, or using large amounts of disk space, for personal use.

- To ensure security, avoid the spread of viruses, prevent external intrusion and data loss, internal users access external services through a combination of firewalls and other security devices. Bypassing these Bank security measures is strictly prohibited. Prohibited activities and tools include, but are not limited to:
  - Modifying default desktop security configuration;
  - Downloading, installing or using:
    - password-cracking software;
    - network sniffing/traffic analyzers;
    - personal VPN or proxy avoidance software;
    - personal encryption software;

- Any activity required for legitimate business purposes is allowed as long as it does not violate this policy or any policy in force within the Bank.

- ***Occasional, limited, and appropriate*** personal use of computer and email systems is allowed, as long as such use does not:
  - interfere with the user's or any other worker's performance;
  - have an undue effect on the Bank's systems or network performance;
  - violate this policy or any policy in force within the Bank

- Personal use of computer, internet and email systems is a privilege that may be revoked at any time by the user's Line Manager or other members of the management team.

4.2 Use of Internet

In order to prevent inappropriate use of the internet by users and avoid negative consequences to the Bank in relation to legal obligations, reputation and personnel performance, the following principles must be acknowledged and adhered to:

- Internet use for communication and information purposes with relation to Rabobank activities is considered as an acceptable internet use.

- The Bank reserves the right to monitor, filter and block user internet activity within the framework of authorities granted by law, in order to secure its goodwill and activities and to preserve the availability, integrity and confidentiality of its information systems.

- Users are cautioned that internet content may include offensive, sexually explicit, and otherwise inappropriate material. Even innocuous search requests may lead sometimes to sites with highly offensive content.

- Although measures are implemented to protect and limit user browsing and email content, due to the nature of the Internet, the Bank cannot be held responsible for material viewed or downloaded from the Internet nor for the safe keeping or transport of any personal details that are sent over this medium e.g. address or credit card details to online vendors.

4.3 Use of Rabobank Supplied Computers and Portable Devices

Following controls are mandated in order to protect the Bank's computers and information systems from harmful software and to ensure their security, to prevent use of unlicensed software, to detect security risks caused by such software:

- The Bank absolutely prohibits users from installing any software on any computer provided by The Bank. All software, however acquired, must be installed by the IT Department only, and in accordance with licensing laws and internal change management procedures. Prior to its installation, all software will be tested for both viruses and functionality with the Bank IT infrastructure.

- Users must not illegally copy material protected under copyright law or make that material available to others for copying. Users must not agree to license or download any material for which a registration fee is charged. It is the sole responsibility of the IT Department to purchase software on behalf of the bank.

- Users who have been provided portable laptops, tablets, smart phones and similar portable devices are responsible for ensuring the continued security of such devices, by regularly connecting them to the Banks network (at least once per month) or presenting them directly to the local IT department. This will ensure security updates and other software programs are kept up to date. **Note: failure to keep your device up to date in this way may result in it being automatically disabled and/or blocked from the Rabobank network.**

- Bank provided portable devices (including laptops) must be secured by anti-theft cables when left for extended periods or secured in locked cabinets.

- Unless suitably encrypted with an appropriate mechanism, complex passphrase and/or key, it is prohibited to keep sensitive confidential information in any portable device. Please confirm with your IT department whether your device has inbuilt encryption or if other measures need to be taken.

- Cases in which any Bank laptop or other portable computer equipment is stolen or lost are considered as potential security breaches and must be reported immediately to the IT service desk.

- The Bank absolutely prohibits the connection of computers provided by Rabobank to any external network for personal use.

4.4 Use of privately-owned computers and devices

- The use of privately-owned computers and devices for the bank's business purposes is allowed on an occasional basis and is subject to approval by the Local Management.

- Users are responsible for the security of the Bank's information at all times and must take all appropriate steps to protect it.

- In particular, the Bank's information must only remain on the privately-owned computer or device for the duration required to meet the business purpose, and must be adequately removed afterwards.

- The Bank absolutely prohibits the installation of any software belonging or licensed to the Bank on any privately-owned computer or device, or on any computer or device not belonging to The Bank.

- The Bank absolutely prohibits the connection of privately-owned computers and network devices to the computer infrastructure of The Bank.

- The connection of privately-owned mobile devices to the Bank's computer infrastructure may be considered (e.g. To Rabobank Guest Wi-Fi networks), but this is subject, in all cases, to the approval of the Local Management who may impose technical constraints on the privately-owned device, prior to authorising the connection.

4.5 Use of E-mail

In Rabobank, the following e-mail security standard apply:

- It is the responsibility of the users to determine, before sending, the sensitivity of the information being sent across inherently insecure data communication media, like the public Internet.

- Users are responsible for protecting sensitive Bank information when sending them across inherently insecure data communication media, like the public Internet.

- In particular, users must NOT forward sensitive commercial or personal information from their internal mailbox to a personal external mail account at an Internet Service Provider or web based system. [Where required to work on something from home, users should contact IT support for details of the multiple secure remote access options]

- Protecting sensitive Bank information must involve a combination of compression, encryption or password-protection techniques.

- In any doubt, users must contact the IT Service Desk or seek alternative ways to exchange the information.

- Users must be aware that similar risks may exist when using the internal mail service. Users should password protect attachments that contain bank sensitive information.

- The Bank absolutely prohibits users from sending or forwarding messages that contain offensive language and/or defamatory, threatening, harassing, obscene, pornographic or otherwise offensive material.

- The Bank absolutely prohibits users from sending or forwarding messages that disclose personal or confidential information on others, (staff members, customers and third parties) without authorisation.

- The Bank absolutely prohibits the use of any corporate email address to exchange information with any external service where the name of the Bank could be misrepresented Please contact the Legal Department where authorisation is required from a staff member, customer or third party.

4.6 Use of Social Media

- Users who participate on behalf of Rabobank on social media need to be recognizable as such and communication needs to be limited to subject matter that the employee is responsible for. Official points of view of Rabobank should only come from the department who is responsible for the Communication & Corporate affairs. (Note: For further information, there is a separate Rabobank Group wide guideline on how to handle social media and digital networks).

4.7 Use of Cloud storage

- Users must only store and share Bank confidential information using cloud services if these have been explicitly approved by the Local/Regional security officer.

4.8 Clear Screen and Clear Desk

General workplace information security standards, required from Users on a daily basis, are listed below:

- All confidential documents and data storage devices including important data (CD, DVD, USB/flash disk, etc.) must be kept secured when they are not used or out of working hours. If there is not a safe or specific lockable cupboard, the room in which they are kept should be locked. Critical information should be protected not only from unauthorized access but also from external effects which can result in the permanent loss such data (fire, flood, etc.). Please speak to your local facilities team for suitable options such are fireproof safe or offsite archiving.

- Password protected timeouts must be enabled for all portable devices containing Bank data (laptops and tablets, smart phones etc.)

- Computer screens should be positioned in such a manner to prevent unauthorised people from viewing any Bank confidential information displayed. (User screens must not be clearly visible to the public from outside of the office/branch)

- If you notice an unattended and unlocked workstation of a colleague, please simply lock this for them.

Tip: Pressing the Windows Logo key + "L" is the shortcut to quickly lock a session

- No authentication details (User IDs, login accounts or passwords) must be written down and/or visible anywhere in the workplace.

- Work areas must be left in a clean and tidy manner outside of working hours.

- Presentation content and equipment such as flip-charts, handouts and white boards should be removed or wiped when no longer needed.

- Areas in which data storage devices are placed shall be kept in closed and locked manner all the time.

- Confidential documents, when no longer required, should only be disposed of in a secure manner. Either directly in a secure "crosscut" shredder or placed in marked and locked confidential bins for subsequent contracted secure disposal.

5 Abuse or Misuse

Due to the nature of the Bank’s business and our fundamental reliance upon computer systems, any abuse or misuse of the above provisions may result in disciplinary action being taken according to the local disciplinary procedure. Where the misuse is deemed to be of a serious nature, it will be treated as gross misconduct and an employee may then face dismissal. Other workers, working for the Bank but non-employed by the Bank, will have their contract for services terminated immediately and legal proceedings may ensue, depending on the terms of the contract.

6 Responsibility

All those persons referred to within the Scope of this policy are required to familiarise themselves with the policy and to adhere to its terms and conditions.

The IT Department is responsible for the implementation, support, and operational security of all the Bank’s IT systems.

In case of any doubt regarding the application or interpretation of this policy, Users must seek advice from the IT Department, or the Local/Regional security officer prior to any action being taken.

The Local Management, supported by the Local/Regional Security Officer is responsible for ensuring a consistent and adequate level of security within the Bank in compliance with Rabobank Global Security policies.

The Local/Regional Security Officer has the responsibility for ensuring the maintenance, regular review and updating of this policy. Revisions, amendments or alterations to the policy can only be implemented following consideration and approval by the Local Management.