Information Management Policy (former Computer Policy)

Issuer	ExCo
Author	Chief Information Officer
Approved by	CFO
Issue date	October 26, 2015
Revision history	Replaces "Computer Policy" of 2002
Publication via	BCnet

Limitations and Disclaimer

This Policy is the Company's general guideline and management reserves the right to apply different terms, as determined in management's sole discretion. This policy can be changed at any time, with or without notice by the employer. Nothing in the policy is meant to alter the at-will nature of the employment relationship. Nothing in this policy shall apply to the extent it would be inconsistent with any applicable law.

At the time of publication of this Policy, Telecommunications and Data Privacy/Protection laws and practice are dynamic and are expected to continue to develop. Management reserves the right to apply a more stringent Policy/practice in specific countries.

Content

1 Purpose and basis of this Policy

The principal goals of this Policy are data integrity; access security and IT asset protection.

Barry Callebaut wishes to make available to employees the most appropriate information processing devices (desktops, laptops, tablets, smartphones), communication services (mobile & fixed telephony, e-mail, voicemail, instant messaging, 3G/4G mobile data access cards) and applications (Google, SAP, salesforce.com etc) in accordance with functional needs whilst considering available budgets.

In order to protect this environment, Barry Callebaut establishes rules pertaining to all Company information systems and data. This document describes the Policy and practice to be followed by all Barry Callebaut users of such devices, communication services and applications.

Any offence against this Policy can lead to disciplinary measures and, as the case may be, legal action taken by Barry Callebaut. In addition, attention is drawn to Barry Callebaut's Code of Conduct and Social Media Guidelines.

2 Addressees of this policy and local implementation

This document describes the policy and practice to be followed by all Barry Callebaut employees. Where for local practice or regulatory reasons this Policy is not directly

applicable to employees, the policy or its content shall be incorporated into the respective local regulations.

3 Specific rules

Tools

3.1 Supplied IT tools remain property of Barry Callebaut

Barry Callebaut provides IT tools to its employees that enable them to perform their jobs in accordance with their instructions and responsibilities. These tools and any data stored thereon in any way, mailed or received by them, are and remain the property of Barry Callebaut. Barry Callebaut may, within the boundaries of applicable legislation, decide how to act with these tools and with this data. IT tools should be used in the manner of good housekeeping and with the same level of care as employees would reasonably treat their own property. Employees who lose or damage equipment must inform the IT Department immediately and may be asked to reimburse replacement costs.

3.2 Office devices and telecom services are for business purposes

Employees shall not misuse Barry Callebaut devices and telecom services for personal use, and shall ensure that substantially only business-related information is stored or received on or mailed from these tools. Incidental and moderate private use is tolerated: for example, when travelling abroad, use of a Barry Callebaut mobile phone is allowed to contact e.g. family. Employees will not misuse the Barry Callebaut electronic mailing system for private reasons, and will discourage third parties from sending non-business-related e-mails.

3.3 Use of privately-owned devices ("BYOD" - Bring Your Own Device)

Barry Callebaut may allow employees to access data stored on company-owned applications with certain devices, even if these devices are not company property (e.g., private smartphone or tablet). Although employees may access, modify or generate data stored on company-owned applications via a privately-owned device, such data remains property of Barry Callebaut. The IT Department will issue periodic guidance and support in this area. It is obligatory to declare the use of a personal mobile device with your IT Department, so that the device can be set up by the IT Department in our "Mobile Device Management" platform for reasons of data security. It is forbidden to use private e-mail for Barry Callebaut business purposes in view of e.g. risk of loss or disclosure of confidential data. In case an employee wishes to install/connect a personal peripheral device (e.g. printer at home) to a device provided by Barry Callebaut, assistance must be sought from the local IT department.

Although employees may access, modify or generate data stored on company-owned applications via a privately-owned device, access to Barry Callebaut network, systems and/or application via privately-owned devices can be more limited than with Barry Callebaut owned devices. When using a privately-owned device, the employee will ensure compliance with all required licenses for the applications installed. Barry Callebaut cannot acquire, install or maintain application licenses for privately-owned devices.

Upon leaving Barry Callebaut, employees using a privately-owned device may be asked by the IT Department to wipe all data from the device in order to ensure deletion of confidential or sensitive company data.

Barry Callebaut, as an organization, is always in control – the enterprise mobility strategy can never be dictated (or limited) by the capabilities (or limitations) of the BYOD platform. Barry Callebaut has full control over the default system behavior and should be able to define and control how it manages its BYOD implementation. For example, while a BYOD solution provider may offer several options to address the issue of jailbroken devices, including blocking and/or removing all or specific applications or profile types, and forcing a full device wipe or device check-in, it is up to Barry Callebaut to decide in those cases, whether it wants to remove specific resources or do a full device wipe.

Data / Access

3.4 Protect log-on credentials

Every employee receives a user-identification number and a password to log on to computers and the Barry Callebaut applications, and must keep them "personal" and "confidential".

3.5 Barry Callebaut may access all business-related information

As an employer, Barry Callebaut has the right and duty to follow up on the work and progress of its employees and their compliance with laws and company policies. In the interests of the company, the progress of activities or the continuity of an employee's job, the company may access all business-related data stored on any of the aforementioned devices. Under normal circumstances the employee will be informed prior to company access of devices. Data on Barry Callebaut provided devices may only be checked within the boundaries of local legislation, if misuse is suspected and if the Group General Counsel and/or Head of Global Human Resources authorize this procedure.

3.6 Unknown data will be removed without accessing it

For reasons of security, employees will remove all mail received from unknown or unrecognizable sources immediately from their workstations, and will not open or distribute email attachments from unknown sources. Barry Callebaut may remove

privately-installed non-compliant or non-standard data, software or applications which are deemed unnecessary for job performance.

Applications / Software

3.7 Internet access will not be misused for company or private purposes

Barry Callebaut adopts a liberal internet access policy, e.g. social media use is permitted in BC offices subject to more stringent local regulation. However, employees will not misuse the Internet, and acknowledge that all websites visited through Barry Callebaut devices (laptops, desktops, tablets, smart-phones) will be registered by the IT Department. At no time is an employee allowed to download files from the Internet from sites which are not trustworthy or which contain offensive or illegal content. When in doubt, contact the local IT Department. The group or local IT Department may block access to websites with inappropriate or offensive content, or to websites not related to company activities, while working in Barry Callebaut offices.

3.8 Software installation with active participation of local or corporate IT

In case an employee wishes to install software for private use on a Barry Callebaut device, the employee shall seek permission and participation of the local or corporate IT Department. Employees may not create, install, copy, distribute or use software in violation of copyright and/or software agreements or applicable country or state laws.

3.9 No illegal or offensive activities are allowed with company devices or telecom services

At no time are employees allowed to use Barry Callebaut company resources for illegal or offensive activities. Illegal or offensive use includes, but is not limited to, access to or distribution of pornography, discriminatory or defamatory statements, threats, harassment, theft, and unauthorized access.

4 Monitoring and reporting

This policy is issued by the Chief Information Officer following review and approval by Head of Global HR and the General Counsel, and is implemented and controlled by IT and HR teams.

October 26, 2015

Steven Vandamme
Chief Information Officer