Information Systems Acceptable Use Policy

Number:	**GPP55-10 GL/en**	**Distribution:**	**Global**
Owner:	**Chief Security Officer**	**Status:**	**Current**
Effective:	**12/28/2015**	**Superseded:**	**N/A**
Comments:	**Migration of DBDPOL01 to New Approved Format**		

Table of Contents

1 PURPOSE

This Information Systems Acceptable Use Policy (the “Policy”) and its supporting standards set forth the acceptable uses of the computer systems of Diebold, Incorporated and its worldwide subsidiaries and affiliates (“Diebold” or the “Company”), and also describe various security measures that will ensure that Company Information Assets (as defined below), whether stored or transferred via any electronic means (e.g., Internet, intranet, email, telecommunications equipment, etc.) are properly controlled and protected.

2 SCOPE

All associates of Diebold and other persons who are authorized by the Company to access Company Systems are responsible for the proper use of such systems and the security of

the Company Information Assets stored on them. This includes, but is not limited to, all documentation, electronic data, hardware, and software necessary for the Company to carry out its own internal business operations. All associates and persons who are authorized to access Company Systems are required to abide by this global Policy.

3 SUMMARY

Access to Company Systems and Information Assets will be limited to authorized users and such users must comply with requirements regarding access, usage, and storage. Company Systems are to be used only for Company business purposes except for certain limited authorized non-Company purposes.

4 DEFINITIONS

Information Assets. Electronic and non-electronic information or information processing assets owned by the Company or entrusted to the Company, the use of which is necessary to carry out the Company's internal business operations.

Instant Messaging. The exchange of text messages through a software application in real-time.

Company Systems. Includes all the computer hardware, software, and communications capabilities provided by the Company to transmit, receive, and store information electronically, including but not limited to email, voicemail, programs, and data.

Objectionable Information or Objectionable Material. Anything that is considered offensive, defamatory, obscene, or harassing, including, but not limited to, sexual images, jokes, and comments, racial or gender-specific slurs, comments, images or jokes, or any other comments, jokes, or images that would be expected to offend someone based on their disability, age, religion, marital status, sexual orientation, political beliefs, veteran status, national origin, or ancestry, or any other category protected by law.

Personal Identification Information ("PII"). PII is information which can be used to identify, contact, or locate a single person uniquely and reliably.

Smartphone. Is an electronic handheld device that integrates the functionality of a mobile phone, personal digital assistant ("PDA"), or other information appliance.

Trade Secrets. Includes but is not limited to a practice, data, process, design, instrument, know-how, pattern, information about suppliers or customers, or a compilation of information, owned by the Company or which has been entrusted to the Company by a third party, which is not generally known publicly and which can be used to obtain an advantage over competitors and/or which provides the Company with actual or potential economic benefit.

User. Any individual or entity authorized to access any Company Systems.

5 REQUIREMENTS

5.1 System Usage

Company Systems are the property of the Company, including all the information received, sent, accessed through use of, or stored on a Company System. Company

Systems are to be used to access Company information and other data, to communicate with Company associates, Company partners (e.g., suppliers, distributors, vendors, etc.), and customers. Company Systems are provided for the Company's information and operational needs, and to facilitate more efficient internal and external communications. The use of Company Systems by employees and others who are authorized to access them is restricted to only Company business except for certain limited purposes as described in this Policy. All use must comply with applicable laws to maintain the security and effectiveness of Company Systems and Information Assets. Associates and others authorized to use Company Systems and Information Assets must be aware that the negligent or improper use of these systems may put the Company and them at risk.

Company Systems may be used by associates for incidental, insignificant personal use during times when the associate should not be working (for example, a lunch period or authorized break time). Such use must be otherwise in accordance with this Policy, and on the basis that anyone accessing the Company Systems for personal use acknowledges and accepts that use of Company Systems is subject to the terms of this Policy, such use will be monitored and that such monitoring may include monitoring personal use. The Company will comply with all applicable laws regarding the privacy of any user with regard to personal use of Company Systems as permitted by and subject to this Policy. In the event of systematic and/or widespread personal use of the Company Systems in violation of this Policy, the Company reserves the right to amend this Policy to prohibit any and all personal use of the Company Systems.

Abusive, unethical, or inappropriate use of Company Systems is prohibited. Anyone who is authorized to use Company Systems should remember that they may be representing the Company in their actions and are required to comply with the highest standards of professionalism, courteousness, ethical conduct, and compliance with all laws and regulations.

5.2 System Access

Only authorized users may have access to Company Systems. Those authorized users are responsible for all of their logon IDs, passwords, and any authorization codes. Security passwords and other access control devices for Company Systems are required to be kept confidential and are never to be loaned or borrowed. Any security violation or violation of this Policy traced to a logon ID is the responsibility of the person to whom it was issued.

5.3 Ownership of Information and Monitoring

Users are not authorized to store any programs, data or information that is not Company property on Company Systems. Any information, content, data, or works that are created, received, accessed, transmitted or stored on Company Systems, including those on a user's assigned Company computer, on the Company's computer tapes, disks, or other storage media, or that are loaded to a user's computer by accessing Company Systems, are the sole property of the Company.

The Company will periodically monitor and may intercept or audit information or communications on Company Systems. This may be done at any time, with or without notice, for purposes of ensuring that Company Systems are working properly and to

check for compliance with this Policy. Those persons with access to Company Systems should be aware that email and Internet messages and other information that they attempt to delete may still be retained in Company Systems. These deleted items, to the extent they are retained, are also subject to monitoring, interception, ownership and audit by the Company.

The Company uses monitoring devices that are designed to detect activity that may result in the loss of confidential information or service of the Company's systems. The Company also uses software deployed across its system to monitor for viruses, network-based worms, and other malicious programs or malicious activity that could affect the Company's Information Assets. The Company deploys software at the perimeter of its network to record inbound and outbound activity, and to protect the Company's Information Assets. Additionally, devices are deployed at various locations around the Company's network for gathering information from the Company's network for the purpose of troubleshooting connectivity, performance, and similar purposes. All of these devices collect information that is used by Company management to record, analyze, and investigate activities that are detrimental to the Company. All information collected through these measures is the sole property of the Company. The Company will continue to evaluate and implement state-of-the-art processes to maintain the security, efficiency, and effectiveness of Company Systems.

5.4 Confidentiality

Associates and other users accessing or using Company Systems should not assume that their use of Company Systems is private or that communications or information that they transmit, access, receive, or delete through Company Systems are or will remain private. No privacy right exists in any files or data that employees or other persons using Company Systems transmit, store, or access. The use of a Company-provided logon ID or password does not in any way restrict the Company's right to monitor and audit Company Systems or an associate's or third party's use thereof.

Associates and other users who are authorized to access Company Systems are not authorized to access email communications or other data that is not sent to them, or which they otherwise should reasonably know they are not authorized to access. The Company's confidential information and trade secrets shall be preserved in secret and shall not be disclosed or disseminated to employees or other persons who are not authorized by the Company to have access to such information.

5.5 Duty to Protect

Access to Company Systems is a privilege granted to users by the Company which can be revoked in whole or in part at any time by the Company. As such, all associates are expected to ensure the appropriate levels of security at all times. The protection of mobile devices (e.g., laptops, flash drives, Smartphones, removable storage, etc.) is especially important. Those authorized to access Company Systems are responsible and will be held accountable for the security of their assigned Company assets.

5.6 Internet Usage

5.6.1 Exploration

Internet access through Company Systems is provided to conduct Company business activities. Accessing the Internet via Company Systems for personal use is restricted as described in Section 4.1 of this Policy. Excessive personal usage is prohibited and grounds for disciplinary action.

5.6.2 Inappropriate Behavior

Using Company Systems to make abusive, unethical, or inappropriate use of the Company's Internet access is prohibited and considered grounds for disciplinary action. Examples of inappropriate associate Internet use include, but are not limited to, the following:

- Operating a personal business;
- Conducting illegal activities;
- Accessing and downloading objectionable material;
- Soliciting for anything that is not expressly approved by Company management;
- Revealing or publicizing confidential information or trade secrets;
- Representing personal opinions as those of the Company;
- Making or posting indecent remarks;
- Downloading or posting copyrighted materials without authorization;
- Providing information about, or lists of, Company associates to parties outside the Company;
- Revealing your account password to others or allowing use of your account by others. This includes family and other household members when working off-site.

5.6.3 Transmission of Sensitive or Protected Information

Transmitting Company-sensitive information (e.g., anything other than that denoted as Public, such as Secret, Confidential, or Internal Use Only information) over the Internet without prior authorization or without using reasonable security measures (such as encryption) is prohibited.

5.6.4 Storage of Sensitive or Protected Information

Storage of Company-sensitive information or trade secrets on non-Company assets is prohibited. Non-Company assets include, but are not limited to, home computers and personal flash drives.

5.6.5 Use of Cloud-Based Storage

The use of cloud-based storage services is strictly prohibited for the storage or transfer of Company information, unless approved by Global Risk and Security. Examples that are included in prohibited services, but are not limited to, are:

- Amazon Cloud Drive
- Carbonite Online Backup
- iCloud
- Dropbox

5.6.6 Web Sites

Company Systems routinely prevent users from connecting with certain non-business web sites. However, the ability to connect with a specific web site does not in itself imply that users are permitted to visit that site while using Company Systems. Using Company Systems to visit web sites that contain offensive or objectionable material is prohibited.

Unless previously approved by Global IT and Corporate Communications, users are not permitted to use Company Systems to produce web pages or sites that reference the Company or its affiliates, masquerade as the Company, or in any way disclose non-public information about the Company. Company Systems shall not be used to host web sites that harass associates or other persons through the transmission of objectionable material or illegal materials. Users are not permitted to host personal web sites on Company Systems or use Company logos or trademarks on their personal sites. All Company-sponsored web sites require approval by Global IT and Corporate Communications and their content shall follow change management procedures.

5.6.7 Representation of Company Positions and Personal Opinion

Using Company Information Assets to participate in blogging, discussion groups, mailing lists, chat sessions, or other interactive Internet offerings that discuss the Company or its business operations, whether directly or indirectly, unless expressly approved by Company management, is prohibited. If such discussions are authorized by Company management, users should clearly state when opinions expressed are their own and not those of the Company.

5.7 Intranet Usage

5.7.1 Posting to the Intranet

Posting Company-sensitive information or trade secrets on the Company intranet is prohibited unless approved by appropriate Company management.

5.7.2 Intranet Usage

The Company intranet should be used only for Company business-related purposes. Forwarding information on the Company Intranet to unauthorized third parties is prohibited.

5.7.3 Intranet Connection

All requests for connections to the Company intranet shall be submitted to Global IT. Global IT will approve all intranet servers and access.

5.8 Software Usage

5.8.1 Software Acquisition

Properly licensed copies of software will be provided to all users who the Company considers have a need for such software. All requests for software, including upgrades, shall be submitted to Global IT, or authorized Company functions. All software acquired by the Company shall be purchased through Global IT or authorized Company functions. Software acquisition channels are restricted to ensure the Company has a complete record of all software that has been purchased for Information Assets and can register, support, and upgrade such software. Purchasing software for use on Company Systems through user corporate credit cards or personal expense reports is prohibited.

5.8.2 Software Installation

It is the policy of the Company to respect the rights of third parties who supply computer software to the Company and to abide by the terms of all software licenses to which the Company is a party, therefore:

- Knowingly using software for which the Company lacks the appropriate license is prohibited.
- Installing unauthorized software that prevents the Company's authorized representatives from accessing, operating, or recovering Information Assets is prohibited.
- Loaning or giving to anyone any software licensed to the Company is prohibited.
- Using or distributing personally-owned software on Company Systems is prohibited. Such software threatens the integrity and security of the Company's systems and Information Assets.
- The downloading of unapproved software from external sources (e.g., from an external network or a bulletin board, a vendor's product or demo, vendor's diagnostic/maintenance package, client, customer, memory sticks, mobile phones, etc.) using Company Systems is prohibited. Only Global IT or other authorized Company functions can approve downloading of software from external sources.

- If you become aware of the use or distribution of unauthorized software, you should notify your manager or Global IT.

- Unauthorized software or data on Company Systems is subject to immediate removal without notification.

5.8.3 Security Software

Disabling any security software (e.g., antivirus software) that Global IT has installed and enabled on any system used to connect to Company Systems is prohibited. Also, any system owned by Company personnel or other users to access Company Systems or Information Assets shall have appropriate security software installed. Wiping tools (tools that prevent the retrieval of data or permanently destroy data) are prohibited without written authorization from the office of the Chief Information Officer.

5.9 E-mail Usage

5.9.1 Personal Use of E-mail Systems

Use of the Company's email system should be consistent with the Company's business purpose, and personal or non-business use is restricted as set forth in Section 5.1 of this Policy.

The Company's email systems shall not be used to create, distribute, or receive any disruptive or objectionable material, including discriminatory or offensive statements. Associates who receive any emails with this content from any Company associate should report the matter to their management or Human Resources ("HR") representative.

5.9.2 Usage Restrictions

Using the Company email systems to produce or distribute chain mail, SPAM, propagate email hoaxes, engage in non-Company business activity, or make solicitations for personal gain or for outside organizations is prohibited. All electronic communication with customers and suppliers is to be performed through internal Company email accounts. Contractors will not be provided with Diebold email accounts or addresses.

5.9.3 Transmitting Sensitive Material

The Company's email systems shall not be used to transmit or receive sensitive information or trade secrets without authorization. If such information is transmitted, appropriate protective measures shall be employed, such as encryption.

5.9.4 Retention and Destruction of Archived E-mail Messages

Email correspondence shall be retained and disposed of in accordance with the period outlined in any applicable policy and in compliance with all applicable laws.

5.9.5 Outlook Web Access

Outlook Web Access ("OWA") is a web client that allows Company associates to access email from outside the Diebold network. The use of OWA is subject to the email usage policies outlined in this Policy.

5.10 Virtual Private Network ("VPN") Remote Access

5.10.1 Personal use of VPN Remote Access

This Policy applies to remote access connections used to do work on behalf of the Company. VPN allows Company associates to access the network from a remote, non-Company location for business purpose only. The use of VPN remote access should be consistent with the Company's business purpose, and personal or non-business use is restricted as set forth in Section 5.1 of this Policy. Users should ensure that their remote access connection is given the same consideration as the user's on-site connection to the Company's network.

5.10.2 VPN Usage

All Company associates and other persons authorized to utilize VPN remote access are to use Company approved devices and software to access the Company's network.

5.11 Unauthorized Security Activity

The following activities are examples of violations of this Policy:

- Introduction of malicious programs into Company Systems (e.g., viruses, worms, Trojan horses, email bombs, etc.).
- Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing unauthorized data, unless these duties are within the scope of regular their duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
- Penetration testing, port scanning or security scanning is prohibited without prior approval from the Chief Security Officer ("CSO") or Vice President, Internal Audit is granted.
- Executing any form of network monitoring that will intercept data not intended for the associate, unless this activity is a part of the associate's normal duties.
- Circumventing user authentication or security of any host, network, or account.
- Interfering with or denying service to any user (for example, denial of service attack), except as directed by management of the Company.

- Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/intranet/extranet.

5.12 Technology Usage

5.12.1 Non-Company Devices

Connecting non-Company computing devices internally to the Company intranet without prior approval from Global IT is prohibited. Even non-Company computing devices that are granted access to the Company intranet shall be compliant with all Company IT security requirements. Company devices that have non-standard images (non-standard images may indicate that those systems may not have the latest security software such as firewalls anti-virus software, etc.) from Global IT are prohibited from connecting to the Company intranet.

5.12.2 Wireless Acceptable Use

Guest wireless access will be provided through a segmented network which will only allow access to the Internet. Use of the guest network by associates and others who have master accounts is prohibited.

5.12.3 Instant Messaging

The Company Instant Messaging capability is for business purposes.

Using Instant Messaging on Company resources for creating, receiving, sending, viewing, or storing objectionable information or material is prohibited.

6 CONTACTS

If you have any questions or comments regarding this Policy, please contact the Chief Security Officer (GlobalRiskandSecurity@Diebold.com).

If you are aware of any violations of this Policy, it is your duty to report that violation to management or through the EthicsPoint hotline, which is available by telephone at 1-866-ETHICSP (1-866-382-4277) and online at http://www.ethicspoint.com.

7 EXCEPTIONS

- Any exceptions to this policy should be submitted through the access request tool.
- Exceptions must be approved by Global Risk and Security prior to implementation.

8 RELATED DOCUMENTS

TITLE	GPP NUMBER
Code of Business Ethics	GPP10-01
Confidentiality and Disclosure Policy	GPP10-06
Global Risk and Security Policy	GPP55-01
Information Classification and Handling Policy	GPP55-05

9 HISTORY

REV	DATE	COMMENTS	BY
1	7/2008	Original Release (DBDPOL011-1)	Chief Security Officer
2	6/2009	Updated Enterprise Security email address (DBDPOL011-2)	Chief Security Officer
3	2/2011	**Updated and revised** organization name to Global Risk and Security, added VPN information, revised Section 3.6.3, and general updates. **(DBDPOL011-3)1/2012**	Chief Security Officer
4	1/2012	Updated ownership to Chief Security Officer (DBDPOL011-4)	Chief Security Officer
5	10/2012	Updated to include appropriate use of cloud storage technologies. (DBDPOL011-5)	Chief Security Officer
6	4/2013	Reviewed for content (DBDPOL011-6)	Chief Security Officer
7	7/2013	Removed termination clause (DBDPOL011-7)	Chief Security Officer
8	9/2014	Reviewed	Chief Security Officer
9	10/2014	Updated section 3	Chief Security Officer
10	11/2015	Reviewed for content	Chief Security Officer
11	12/2015	Migrated to new policy format	Global Policies & Procedures Committee