

E-mail & Internet Security Policy

Version: 1.3

This document contains proprietary or confidential company information.
© Copyright Headhunter System Limited



Table of Contents

1. Overview	3
2. Purpose	3
3. Scope	3
4. Email Sending and Maintenance Guidelines	3
5. Unacceptable Use	3
6. Email or General Data Retention	4
7. Monitoring	4
8. Internet Surfing Guidelines	5



1. Overview

- 1.1. E-mail and Internet communication can involve significant security risks and should therefore be handled according to Gravyty's relevant security guidelines.
- 1.2. This policy details the most secure manner for sending e-mails and surfing the Internet to prevent the potential compromise of Gravyty's information.

2. Purpose

- 2.1. The purpose of this policy is to define the method and conditions for use of the Internet and of Gravyty's e-mail services by computers linked to the company network.

3. Scope

- 3.1. This policy applies to Gravyty's e-mail and Internet surfing system.


4. E-mail Sending and Maintenance Guidelines

- 4.1. Sending e-mail is equivalent to sending an official company letter by mail. Any letter sent by e-mail must include a signature comprising the sender's name and telephone number.
- 4.2. Forwarding e-mails automatically from the company to an external site is prohibited, since this is liable to result in the transfer of sensitive or classified e-mails out of the company network without the sender's knowledge.
- 4.3. Spam should be deleted immediately from an employee's inbox. Forwarding spam (including chain letters) is strictly prohibited.
- 4.4. Opening e-mail attachments is permitted only when the employee recognizes and can vouch for its source.

5. Unacceptable Use

- 5.1. Gravyty's e-mail system shall not be used for the creation or distribution of any disruptive or offensive messages, including but not limited to comments about race, gender, hair color, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs or national origin.
- 5.2. Sending unsolicited e-mail messages is prohibited, including chain letters, virus alerts, joke e-mails, junk mail or other



- 
- advertising material to individuals within Gravyty and outside it, whether they specifically request such material or not.
- 5.3. Any form of harassment via e-mail, telephone or paging, whether through language, frequency, or size of messages, is strictly prohibited.
 - 5.4. Unauthorized use or forging of e-mail header information is strictly forbidden.
 - 5.5. Soliciting e-mails for any other e-mail address other than that of the poster's account, with the intent to harass or to collect replies, is forbidden. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type is forbidden.
 - 5.6. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam) is forbidden.
 - 5.7. Personal Use – Using a reasonable amount of Gravyty's resources for personal e-mails is acceptable, but non-business-related e-mail must be saved in a separate folder from work-related e-mail.

6. E-mail or General Data Retention

- 6.1. All e-mails are to be retained until the departure of a Gravyty employee or the retention requirements of applicable law, the later of the two.
- 6.2. The Gravyty CFO shall determine the retention policy of departing employee's e-mail.
- 6.3. Special attention is to be paid to the deletion rights and "right to be forgotten" of data subjects, which will override all Gravyty internal policy as applicable by law. See the Data Protection and Privacy Policy herein.

7. Monitoring

- 7.1. The IT Management Group may monitor e-mail messages, as well as any data held on Gravyty systems, without prior notice. Notwithstanding, Gravyty is not obliged to monitor e-mail messages.



8. Internet Surfing Guidelines

- 8.1. Internet usage is intended for work purposes only.
- 8.2. Use of the Internet from the company network is intended solely for the work of authorized employees.
- 8.3. Downloading material from the Internet is permitted only under information security restrictions and limited to material that does not infringe on copyright laws and is required for work purposes.
- 8.4. Downloading and installing shareware or freeware is permitted only after information security approval has been received and within the framework of the terms of use and payment for that particular software.
- 8.5. Downloading and sharing unlicensed music and movie files (not limited to MP3 or AVI files) is strictly forbidden. Such downloads may infringe on copyright laws and pose a security risk by endangering the company's information via possible malware contamination and spreading.
- 8.6. No direct connections from the Internet to sensitive data is permitted. All traffic must pass through a firewall and make use of an authentication mechanism.
- 8.7. Browsing unreliable Internet websites or websites containing pornographic material or other improper material is strictly forbidden.
- 8.8. Browsing, exporting or importing materials that are or could be in any way considered pornographic, obscene, offensive (whether from a sexual, racial, political, religious or any other perspective), defamatory or of a criminal or subversive nature, is strictly forbidden.
- 8.9. Clicking on unreliable links while surfing is strictly forbidden.
- 8.10. Web access is not to be provided to websites that can be categorized as follows:

Adult or explicit	Chat	Criminal skills
Drug alcohol or tobacco	Gambling	Games
Glamour/intimate apparel	Hacking	Hate speech
Personals & dating	Usenet	Violence
Web-based mail	Weapons	