RF Results LLC

# Email Usage Policy

| | |
|---|---|
| Document Number | ISP-13-009C |
| Version Number | 1.0 |
| Document Location | Information Security Repository |
| Document Owner | RF Results LLC |
| Approval Date | 10 May 2018 |
| Compliance Date | 10 May 2019 |
| Date of Last Review | 10 May 2018 |

# Scope

All RF Results LLC Staff and personnel with access to corporate email whether they be permanent or temporary, employees or vendors or partners, must comply with this policy.

# Rationale

The motive of this email usage policy is to make all its users privy to what the company deems as acceptable and unacceptable behaviour when using corporate email. Following this policy will allow its users to safeguard themselves and the company against unauthorized data distribution or access, prevent security threats such as viruses or compromised files from affecting company systems and hence damage the commercial interests of the company.

# Overview

Electronic mail is used in almost all industries including RF Results LLC as it is an important source of communication between various organizations. Therefore, a framework is required to guide the users on effective use of the company emailing system while at the same time maintaining the commercial interests of the company.

# Defining User Behaviour

## I. Inappropriate Use

Employees must not use corporate email:

- If they do not have authorized access.
- To send out marketing or confidential information of the company which is not authorized.
- To transmit abusive, controversial, hateful, or anti-discriminatory content.
- To transmit pornographic content.
- To share content that is subject to copyright.
- To purposely spam other people's email accounts.
- To engage in illegal activities.
- To sign up for websites or services that offer illegal activities or have major ethical issues in how they operate their company.
- To attach file sizes that are larger than 100MB to avoid excessive strain on company resources. Furthermore, even if the company allows the transmission of larger files, the receiver may not have the same capabilities and may not be able to access such large files. Additionally, certain file types which are known to carry viruses are also

forbidden and cannot be attached through corporate email. Thus, it is favorable to send larger or forbidden file types through the company's file transfer service.

- Users must not use the corporate emailing system in such a way that it uses excessive resources (i.e. Attaching or downloading large file sizes repeatedly) and thus disrupting performance for other users. If a task requires it, the user must contact the IT support desk for assistance who will then allocate the required resources to the user.

## II. Appropriate Use

Users must use their access to corporate email for the following purposes only:

- Primary purpose should be for company related purposes. Use of corporate email for personal use is allowed if it for the purpose of advancing the company's commercial interests. These include:
    - Registering to online courses, applications, or websites.
    - Downloading professional, educational, eBooks, guides useful materials for from safe and trustful site.
- Provide or advertise corporate email address to other organizations in order to advance the company's commercial interests.

Users with access to corporate email must ensure that:

- Any data in emails that are termed as company records must be retained according to the company's **asset classification and management policy**.
- A formal style of communication be used while using corporate email to communicate with individuals or organizations. Additionally, it is important to be aware that an excessively formal style may seem too tedious for some.
- A disclaimer while sharing confidential information. It must state that confidential content is being shared in the email and that it is intended for use of the named recipient only. The disclaimer must also provide information on how a receiver might respond if they have received confidential informational not intended for them.
- They inform the IT support desk as soon as the user becomes suspicious that accessing a link or an email attachment has compromised the system.
- Emails are responded to within actionable times (< 24 hours). Furthermore, it is also recommended that users with access to corporate email who may be on leave or vacation and hence unable to respond set up an auto responder or auto forwarder with alternate contact details. The user can request assistance from the IT support desk if they require help setting up the above mentioned features.

# Email Signatures

It is recommended that users with access to the corporate electronic mailing system use email signatures while transmitting mail as it portrays a more professional look and thus provides additional positive brand recognition. Furthermore, it provides a quick access to the sender and company's contact information. The contents of an email signature should include the name, title, email address, mobile number of the sender, the company's logo, and website URL. Users requiring assistance in setting up an email signature can contact the IT support desk for assistance. The template for the email signature is provided below:

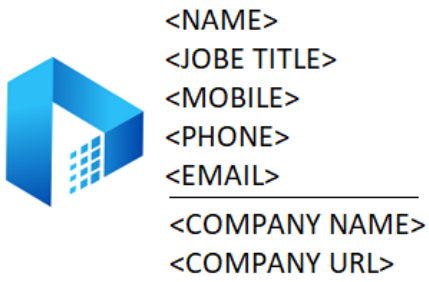


Figure 1: Email Signature Example

# Monitoring and Surveillance

RF Results LLC shall:

- Monitor messages sent or received on corporate email in accordance to the company and the residing government's workplace surveillance laws. While the company does not want to become a censor, this is important to ensure that procedures laid forth in this policy are followed.
- Expect users with access to corporate email to have no expectation of privacy while storing, sending, or receiving data on their corporate email. Email or content received through the corporate electronic mailing system may be shared for other company related purposes in accordance to the company and the residing government's privacy laws.
- Emails may be stored centrally and hence might still be available even after the user deletes them.

# Email Storage and Disposal

Every corporate email account is provided a limited storage space and hence it is recommended to delete unwanted emails. The company's corporate emailing system is not a recommended method of storing information and any company-related records requiring long term storage should be dealt with according to the company's **asset classification and management policy.**

# Incident Handling

It is recommended to delete spam emails. Responding to a spam email will make the emailing system believe that it is actually a genuine address and future emails from the particular address will therefore not be addressed as spam. The block feature can be used to avoid receiving unwanted information. Assistance of the IT support desk should be requested if the user is unable to stop receiving unwanted information or spam emails. The company will investigate all complaints internally and externally thoroughly according to the company's disciplinary procedures but as logs are kept only periodically, it is recommended that incidents are reported promptly.

# Violations and Penalties

Users who do not follow the policy put forward in this document will face strict disciplinary action that may in severe cases lead to the termination of employment. In addition, users may also be personally held liable for any losses and/or damages caused by the violation(s) due to their conduct. If a user is hesitant as to whether a procedure constitutes acceptable corporate email usage, they should contact their supervisor for assistance.