IT Division Documentation

Version – 2 Revision Date: 4/12/2023

IT – Email Acceptable Use Policy

[This policy contains the official IT Email Acceptable Use Policy]

TABLE OF CONTENTS

1. SUMMARY

The Fond du Lac Band makes email available to its employees where relevant and useful for their jobs.

The Email Acceptable Use Policy will describe the rules governing company and personal email usage, and how users are expected to behave while using company email addresses. It is also designed to be read alongside the Computer Use Policy, which can be found on the IT Division page.

The elements of the Email Acceptable Use Policy will clearly define what authorized users are allowed and not allowed to do when using their company, and personal email addresses.

2. SCOPE

The Email Acceptable Use Policy applies to all employees, consultants, and partners that have received a company email address (e.g. johndoe@fdlrez.com). This policy applies to individual as well as departmental email accounts (e.g. servicedesk@fdlrez.com).

This policy applies to use of company email on any device, whether owned by FDL Band or the employee. It also applies regardless of where the company email is accessed and used, whether on-premises or off.

3. AUTHORIZED USERS

Only users that have been authorized to use company email may do so.

Authorization is provided by department leads/heads, and the IT Department. Unauthorized use is strictly prohibited. Company email users may ***not*** give their logins to unauthorized users or share that information with anyone for any reason.

4. EMAIL OWNERSHIP

All forms of email sent, received and archived using a company email address belongs to the FDL Band. FDL Band at any time has the right to access, change or delete email messages without prior notice. Employees must maintain no expectation of privacy when using company email addresses.

5. APPROPRIATE USAGE OF COMPANY EMAIL

Employees can use their company email addresses for work purposes without any restriction. Some examples of business purposes include:

- Official communication with customers, prospects, partners and vendors
- Providing your company email address to potential business contacts met at company events
- Log in to company-owned software
- Sign up for any platforms that will enable professional growth
- Sending sensitive information that must be encrypted by Zix
    - For more information regarding use of Zix, please contact the IT department
- All business-related communication

6. ABUSE AND INAPPROPRIATE USAGE

A company email account may only be used for the aforementioned reasons listed under the heading '***Appropriate usage of FDL email***'. If you have a question on what is acceptable or not, please discuss with your superior or the IT Department.
Examples of employee abuse of company email:

- Use the company email address for illegal, disreputable, and unethical reasons
- Send out unauthorized emails
- Sending out sensitive and confidential data that is not appropriately protected (encrypted). E.g. Protected Health Information (PHI), Personally Identifiable Information (PII) etc.
- Send out offensive and discriminatory messages.
- Signing up for any personal services, such as Spotify, Fitbit, etc.
- Spam coworkers and third parties intentionally
- Exfiltration of data to a personal account (e.g. Forwarding company-only documents to yourself)
- Adding your email to personal mailing lists that do not pertain to company activity
- Opening new accounts on websites that are not related to business

7. USE OF PERSONAL EMAIL

Employees ***must*** refrain from using personal email for anything related to business activity.

Employees must also refrain from accessing their personal email on company equipment. Personal use of personal email should remain on personally owned devices, and should be accessed when appropriate (e.g. during breaks).

If it is not related to business, a personal email ***must be used.*** Some examples include:

- Signing up for personal services, such as Spotify, Fitbit, Netflix, etc.
- Opening new accounts for personal use
- Adding yourself to mailing lists

Examples of where a personal email is ***not*** allowed:

- Communicating with other FDL employees in regards to business activity
- Sending data/information that is business related
- Requesting information that can be deemed sensitive

If a company email user must use their personal email for business purposes, please inform a supervisor or the IT Division so an accurate assessment can be made, and solutions provided.

All FDL email users have access to their company email outside of the facility, and can easily send attachments and reports securely to themselves. They also have the option to use Box (FDL approved file

sharing application) to securely upload documents if they need to be shared. If a Box account is needed, users should contact their supervisor for access.

8. EMAIL SECURITY

Emails are often leveraged by cyberattacks like phishing that can compromise the reputation of the FDL Band. To prevent the risk of cyberattacks, each account holder must:

- Use strong passwords that include a mix of capital and simple letters, numbers and symbols
    - A strong password will likely remain strong in the future (see Password Requirement)
- Must not write down passwords so they are accessible in plain view, or easily accessed by unauthorized parties
- Users must change their password and contact the service desk upon suspicion of a breach or any malicious activities.
    - Use the email web portal or call IT service desk for assistance.

Employees must also be vigilant of unusual emails that may be malicious. Employees are advised to:

- Avoid clicking on links and opening attachments from sources they do not trust
- Be aware of sensationalized subject lines (e.g. You won't believe what you see in this video!)
- Be suspicious of titles that look like the sender simply wants you to click on a link
- Ensure unknown senders are legitimate
- Look for red flags (e.g. poor grammar, unusually high numbers of exclamation marks or capital letters)
- Suspicious order confirmation emails
- Refer to the IT Division with email and security questions and concerns

Potential consequences of a hacked email might include the FDL Band being blacklisted from email services, so emails will not be delivered to various parties.

They might also include more damaging actions such as loss/breach of data, disruption of business operations, and possible legal actions taken against the FDL Band.

9. PASSWORD REQUIREMENT

The following password requirements are enforced.

- Minimum password length: 12 Characters
- Maximum password age: 1 year
- Password history: 4 last passwords
- Meet the following complexity requirements:
    - Not contain the user's account name or parts of the user's full name that exceed two consecutive characters
    - Contain characters from three of the following four categories:
        1. English uppercase characters (A through Z)
        2. English lowercase characters (a through z)
        3. Base 10 digits (0 through 9)
        4. Non-alphabetic characters (for example, !, $, #, %)

10. Non-Compliance of Email Acceptable Use Policy

Failure to adhere to this policy will result in disciplinary action and may impact yearly evaluations.

11. Revision History

This standard shall be reviewed at least once every year to ensure relevancy.

Date	Version	Description of Change	Reviewer
06/01/2021	1	Policy Creation	Nikolai A. Gybin
04/11/2023	2	Formatting Changes: ● Changed each heading to "Heading 1" so that an automated table of contents could be created. ● Numbered each heading, removed redundant spaces between paragraphs. Policy Changes: ● Added the section # 9 "Password Requirement" ● Added bullet # 3 in Section 6	Bishal Thapa

---

Key Details

- Policy Prepared by: Nikolai A. Gybin, Information Security Officer
- Policy prepared on: 02/23/2021
- Approved by: Reservation Business Committee
- Approval Date: 4/21/2021
- Policy Live Date: 6/1/2021
- Next Review: 4/11/2025

GLOSSARY