Document number: OC.40
Document Name: Email Use Policy
Document Owner: Operations Director
Issue Date: 01/05/2024
Current Revision Date: 01/05/2024

Email Use Policy

Objective and Scope

The objective of this policy is to document the protocols when using company emails.

Email is essential to everyday work. Any individual authorised or required to use a Prevision Research email address is required to work within the protocols of use of corporate email accounts.

The intention is to protect our confidential data from breaches and safeguard our reputation and technological property.

Roles, Responsibilities and Authorities

Corporate emails are powerful tools. Authorised users shall use corporate emails primarily for business-related purposes.

The rules and standards outlined in this document are mandatory. As password security is critical to organisational security, a breach of this policy may result in disciplinary action or contract termination.

Roles and responsibilities for this policy are assigned to the Data Privacy Officer Jonathon Power to develop and monitor the policy.

This policy applies to all authorised users including subcontractors. Every individual using a business email takes responsibility for ensuring it is used in compliance with company policy.

Legal and Regulatory

Email usage must consider personal information about individuals, which cannot be provided to third parties without their consent. The email address or personal details of persons or stakeholders and other identifying information must be treated as prescribed by privacy laws.

ISO 27001: Information Security and Privacy Policies / Emails

ISO 27001/2 REFERENCES	ISO 27001: 2022 Clause ID	ISO 27002: 2022 Control ID
Policy		5.1

Email Policy

Prevision Research corporate email users represent our organisation.

Appropriate corporate use of emails.

Authorised email users are able to use the company email system for all company and work-related business.

This includes:

- Communications with current, past and prospective clients and partners.
- Log into software applications where they have been given permission to do so.
- Share their email address for business purposes, including business functions.
- Sign up for online services or information of a professional nature related to business activities.

Personal use of a corporate email address.

Authorised email users are afforded the use of their company email address for restricted personal use. Please be aware that the organisation monitors and may archive emails sent and received from the corporate email system.

This includes:

- Registering for educational purposes.
- Download eBooks, guides and other content for their personal use as long as it does not put others within the organisation at risk, or the content reflects poorly on the organisation.
- Send and receive emails from and to others as long as they do not negatively impact the organisation and the individual is prepared for the content to be subject to monitoring for cyber security risk.

Inappropriate use of corporate emails.

As a Prevision Research representative, you must NOT:

- Sign up for unauthorised, unreliable, disreputable or suspect websites and services. Always seek approval first before adding any website or service to a Prevision Research email address.
- Respond to emails containing material that is offensive, obscene, defamatory, threatening, harassing, bullying, discriminatory, hateful, racist, sexist, infringes copyright, constitutes a contempt of court, breaches a Court suppression order or is otherwise unlawful.
- Use personal email on any social media websites or connections.
- Send unauthorised marketing content or solicitation emails.
- Register for any services not authorised by the company.
- Use inappropriate language, and abusive or discriminatory comments in an email.
- Intentionally spam another person's emails, including those internal to the company.

Email cybersecurity and password management

Emails are typically subject to cyber hacking attacks, including phishing. This can result in confidentiality breaches, virus intrusion and other malware.

- Avoid opening attachments and clicking on links when the content is not adequately explained.
- Be suspicious of clickbait titles.
- Check the email and names of unknown senders to ensure they are legitimate.
- Look for inconsistencies or style red flags (e.g. grammar mistakes, capital letters, an excessive number of exclamation marks.)

Email Use Policy

Email password management

Email passwords must be strong (quality) passwords. This is defined as a password that is reasonably complex and difficult to guess in a short period of time, either through human guessing or the use of specialised software. A pass phrase is considered a form of a password and fits within the same development principles.

As a minimum, a strong password or pass-phrase shall include:

- 8 characters as a minimum that do not form a name, word, slang or dialect e.g. nXp#pd8tUqz
- 12 or more characters if using a mixed phrase e.g. fixdoGbig$orrynot
- Mix of upper/lower case character - English A- Z
- At least one numeric character - 0 - 10
- At least one non-alphabetical character e.g. # % $

Email password change management requires a frequency of change as follows:

- Personal email password: Replace every 30 days.

Email signature

Create an email signature that reflects the company and your role. Include:

- Individual's Name
- Individual's Title
- Company name + link to the company website.
- Phone contact + company address
- Company logo.

Policy review

This policy shall be reviewed by the Directors annually or immediately after a process change or a policy breach is known to have occurred.

Periodic reviews shall take into account feedback from management reviews, regulatory changes and audits. Changes to the policy must be approved by a Director then communicated to all previous persons or organisations with access to the policy. Refer below for the most recent review.