]	Document Number: INS-002987	Revision: 9.0
Product Line / Function: Group IT		Level: Global
Document Type: Standard		

Title:

IT Acceptable Use

Revision List

Revision	Date	Prepared by	Reviewed by	Approved by
1.0	06/11/2015	Lois Lee	Andy Gould	Martin Ogden
Revision Comment: First release within Insight				
2.0	21/03/2016	L Main	Chris Moreau	Martin Ogden
Revision Comment: No change to document content, amendments made to Owner and Reviewer document properties.				
3.0	29/11/17	Chris Dillon	Ross Campbell	Martin Ogden
Revision Comment:				
4.0	14/12/17	Chris Dillon	Ross Campbell	Martin Ogden
Revision Comment:				
5.0	15/12/17	Chris Dillon	Ross Campbell	Martin Ogden
Revision Comment: Spelling error correction clause 6.8				
6.0	12/02/18	Chris Dillon	Ross Campbell	Martin Ogden
Revision Comment: Change of wording for clause 6.8				
7.0	25/03/21	Ross Campbell	Graeme Burrows	Brad Krol
Revision Comment: As per DCR 8721, added expanded section 6 on Passwords. Removed wording on passwords from section 7.				
8.0	12/07/21	Ross Campbell	Graeme Burrows	Brad Krol
Revision Comment: Document changed from Policy to Standard. No change to document content. Minor changes to document formatting made.				
9.0	08/10/21	Ross Campbell	Graeme Burrows	Scott Turner
Revision Comment: Document content revised and document renamed				

Table of Contents

1. Purpose

The purpose of this policy is to establish acceptable use of electronic devices and network resources at Expro in conjunction with its established culture of ethical and lawful behavior, openness, trust, and integrity.

Expro provides computer devices, networks, and other electronic information systems (resources) to meet company mission, goals, and initiatives and must manage them responsibly to maintain the confidentiality, integrity, and availability of its information assets. This policy requires the users of information assets to comply with company policies and help protect the company against damage.

2. Scope

This policy applies to everyone (subsequently called “users” in this document) who handles Expro’s information or has access to its information technology (IT) systems or networks. Users are expected to be familiar with and adhere to the Expro Code of Conduct and to other applicable policies for their locale.

All individuals will be held accountable under this policy, with violations resulting in loss of access to IT systems and/or disciplinary action up to and including termination of employment or termination of their relationship with Expro.

Users learning of violations of this policy or having questions or concerns should notify Group IT, the IT Security Manger, the user’s direct manager, Expro leadership, the Chief Compliance Officer or the Business Conduct Reporting Line (as outlined in the Expro Code of Conduct).

This policy is not intended to contradict any law or grant any rights.

3. Handling of Expro Information

Users are expected to exercise due care when handling Expro information (whether in verbal, written or electronic form) and when using Expro IT systems. For example, users will be diligent to ensure that sensitive conversations are not overheard, that computer screens are not observed, that sensitive papers and electronic media are not left unsecured, and that sensitive papers are shredded rather than being put in the trash.

Wherever possible, sensitive information should be appropriately locked or hidden when work areas are unattended. Computer and mobile device screens must be locked when unattended (requiring a password, PIN or biometric to unlock), and reasonable measures taken to prevent loss or theft of devices, papers and media

Users will not share Expro information inappropriately or without proper approval and must validate the identity of anyone with whom information is shared.

4. Authorized Access Only

Users are expected to use Expro information and IT systems only as authorized. Exceeding or attempting to exceed one's authorized access is prohibited, as is disrupting or attempting to disrupt Expro information or IT systems.

Circumventing, attempting to circumvent or maliciously claiming to circumvent security controls is prohibited, as is the possession of unauthorized tools used for these purposes.

The possession or introduction of malware (such as viruses or keyloggers) is prohibited.

Use of non-Expro remote access technology (such as LogMeIn, GoToMeeting, or VPN software) is prohibited without explicit approval of Group IT.

Only devices authorized by Group IT are to be connected to Expro's IT systems and internal networks (note that use of the guest wireless network does not require Group IT approval).

Repair or disposal of Expro IT devices and media requires approval of Group IT.

Expro information and its IT devices must be surrendered upon termination of employment or the business relationship.

5. Appropriate Content and Behavior

Users are reminded that their conduct must comply with the Expro Code of Conduct and other applicable policies (such as the Anti-Harassment and Bullying Policy and Social Media Policy) including when using Expro IT systems and when using the Internet.

Users are expected to uphold high standards of behavior and not forget that they are representing themselves and Expro.

Communications should be written such that the writer would not be embarrassed if that communication were read aloud in a meeting, at a family birthday party, or in a court of law.

Messages should not damage Expro’s image or reputation, be defamatory, or risk incurring liability. Users are prohibited from broadcasting unsolicited personal views on social, political, religious or other contentious non-business related matters and are not allowed to create, store or send commercial advertisements or solicitations that are not business related.

Users are prohibited from communicating or exposing other people's personal or private information without their permission.

Purposely subjecting others to inappropriate, offensive, distasteful, hateful or explicit content is prohibited, as is purposely creating, accessing, storing or transmitting it.

Communications (such as email) may not remain private and could be used as evidence in a court or by law enforcement.

Users are prohibited from copying, using, publishing, sharing or downloading copyrighted software, media (music, films, pictures, etc.), or materials without permission from the copyright owner. Other violations of copyrights, trademarks, patents, trade secrets or other intellectual property rights or protections are also prohibited.

6. Monitoring and No Expectation of Privacy

To the degree permitted by law, Expro may monitor the usage of Expro's IT assets. This includes monitoring, reviewing and accessing content created or stored on Expro IT systems and content sent or received using Expro IT systems and networks.

Expro employs monitoring by authorized personnel to protect its interests and may do so without prior notice, reasonably and proportionately in accordance with good business practice, and in accordance with local laws. For example, where there is a business reason to do so, the contents of individual mailboxes may be examined by authorized personnel with or without notifying the user.

Information may be provided to third parties such as law enforcement when necessary.

Users should have no expectation of privacy in anything they create, store, send, or receive using Expro IT resources, including personal communications.

Users consent to allow authorized personnel access to and review of all materials created, stored, sent, or received by the user when using Expro IT resources.

7. Accountability for Access and Passwords

Users will be held accountable for use (and misuse) of their Expro issued accounts, passwords, access, information and devices.

Users are not permitted to share accounts, disclose their own password, or disclose or use someone else's password.

Users are encouraged to avoid thinking of a strong password as a cryptic jumble of characters that is hard to remember and hard to type. Instead, users should think of a passphrase. A passphrase is longer, but more like a sentence that is easier for most people to remember and type. For example, the following are good examples of strong and complaint passphrases (but please don't use these exact ones):

- I LIKE cheese sandwiches!
- correct-HORSE-battery-staple
- five divides 15 THREE times

Wherever technically feasible, users should choose long, strong passphrases over short passwords.

Use of a password manager (or password safe/vault) application is encouraged. These applications make it easier to manage multiple passwords by generating strong passwords and storing them securely.

The following are additional requirements for user passwords:

- Do not use the same password across different services, systems or applications. Passwords used on Expro accounts must be different than passwords used on personal or other non-Expro accounts.
- Do not store or communicate passwords in unsecured documents, e-mail or instant messages.
- Do not write passwords down.
- Passwords should not be based on:
    - information that those who know an individual (or can research them) are likely to know (for example, names of spouses and pets, birthdays, favorite sports teams, etc.)
    - Expro, Expro's businesses, words used in the industry, customer names, and so on
    - frequently used weak passwords such as "password", holidays, a month, season or year

Expro IT systems may prohibit the use of certain passwords even where they otherwise meet requirements. Prohibited passwords will include words associated with Expro, common weak passwords, and passwords found in public data breaches.

Where technically feasible, passwords must:

- be at least 12 characters long
- not be the same as a value used for the previous 12 passwords
- be changed every 180 days (or sooner if suspected of being compromised)
- meet complexity requirements, which means the password must contain at least one character from three out of these four categories of characters:
    - lowercase letters
    - uppercase letters
    - digits
    - special characters

The use of biometrics (fingerprints, FaceID, etc.) is permitted when supported by Group IT approved hardware and software.

Multi-factor authentication (also known as two-factor authentication or two-step authentication, sometimes abbreviated MFA or 2FA) is required to be used whenever it is available.

Mobile devices like smart phones and tablets must be secured with a PIN code at least four digits long. This applies to any device that holds Expro information or accesses Expro IT systems, even if it is personally owned.

If there is a reason to believe that someone else knows a user's password or it's somehow been compromised, the user should change their password immediately and contact the IT ServiceDesk. Passwords can be reset using the self-service password reset tool or by contacting the IT ServiceDesk.

8. Use of Non-Expro Services

Expro will provide access to authorized IT services to users based on their role, business need and management approval.

Expro business should be conducted primarily using Expro approved systems.

The use of third party services not authorized by Expro to store or process Expro information or conduct Expro business is prohibited. This includes non-Expro file sharing, instant messaging, e-mail, and other non-authorized cloud applications. For example, users are prohibited from using personal e-mail accounts for Expro business.

9. Use of Non-Expro Devices

Expro will provide appropriate Expro-owned and managed IT devices to users based on their role, business need and management approval.

The use of devices not owned, managed and authorized by Expro to handle Expro information or access Expro IT systems or networks is prohibited, except in the following limited cases:

- Personally-owned smart phones and tablets may be used according to the Mobile Devices section of this policy.
- Devices owned and managed by an approved vendor, partner or customer organization may be used with prior approval from Group IT.
- Non-Expro devices may use the guest wireless network to gain access to the Internet.
- Non-Expro devices (such as home computers and personal smart phones) may be used to access Internet-facing web-based systems (such as Office 365) through a web browser. However, saving Expro information locally or processing Expro information on a non-Expro device is prohibited.
- Use of external or removable media (such as external hard drives and USB sticks), whether Expro- or personally-owned, is discouraged and should be avoided. Approved file sharing methods such as file shares, OneDrive, SharePoint or e-mail is preferred. Due care must be taken when removable media use is unavoidable, and users are encouraged to contact the IT Service Desk for assistance. Encryption should be used where appropriate. Any removable media used to store or share Expro information must be provided to Group IT for secure wiping of Expro information upon termination of employment or the end of the business relationship with Expro.

10. Installation of Software

Users are not permitted to install unauthorized software.

Requests for software that is not already authorized must be directed to the IT ServiceDesk.

Users are not permitted to install, copy or use software in a way that violates software licenses, service contracts, copyrights, trademarks, patents, trade secrets or other intellectual property rights or protections.

If a user is involved in the creation, acquisition, maintenance or administration of a technology system, they must be familiar with the requirements outlined in the Cybersecurity Controls Standard.

All new technology systems or introduction of significant new software must follow the New Technology System Procedure.

11. Acquisition of Hardware

Computer hardware must be purchased using the IT User Request form on the Group IT portal page and must be managed throughout its lifecycle by Group IT.

12. Cybersecurity Incidents

Users must report potential, suspected or confirmed cybersecurity incidents to the IT ServiceDesk or the Cybersecurity Team as soon as possible. This includes the theft or loss of Expro IT assets, compromise of Expro information, unauthorized use or access, suspicious account activity, malware infections, and so on. Users are expected to cooperate fully in any investigations and incident response activities.

13. Mobile Devices

This section covers smart phones and tablets; laptops are not considered mobile devices for the purposes of this section. In some cases, Expro provides users with company-owned devices, while in other cases, users are authorized to use their personally-owned devices for work.

- Expro-owned devices must be enrolled in Group IT's mobile device management (MDM) solution.
- Authorized personally-owned devices that are being used to handle Expro information or access Expro IT systems must be enrolled in Group IT's mobile application management (MAM) solution and optionally may be enrolled in Group IT's MDM solution.
- Devices being used to handle Expro information or access Expro IT systems, regardless of company or personal ownership, must:
- Require a PIN at least four digits long to unlock (biometrics such as Touch ID and Face ID are also permitted)
- Lock the screen after a short period of inactivity
- Enforce device or application encryption
- Have current software updates installed (to applications and the operating system) based on the device vendor's recommendation. This also requires that the device and software be currently supported by the vendor and not be jailbroken or otherwise tampered with.
- Support the ability for Expro to remotely wipe/delete Expro information. Devices enrolled in only Expro's MAM solution are subject to having only Expro information wiped, while devices enrolled in Expro's MDM solution are subject to having the entire device wiped or having only Expro information wiped. Expro retains the right to use this feature at its discretion without prior notice.

14. Personal Use

Users are not permitted to use Expro information for personal use or gain.

Users are expected to use Expro technology assets primarily to accomplish their assigned duties and further Expro's interests. Users are expected to use common sense regarding personal use of Expro's IT assets such as computers, Internet access, telephones and mobile devices. Limited personal use of Expro's IT assets is permitted, provided that:

- It does not violate laws, the Expro Code of Conduct, or other applicable policies;
- It does not run counter to Expro's interests;
- It does not increase risks to Expro, its information or related IT systems;
- It does not negatively impact service to other users or Expro's IT resources;
- It does not violate software license agreements, service contracts, copyrights, trademarks, patents, trade secrets or other intellectual property rights or protections;
- The user does not allow use or access by others (such as friends or family members);
- It does not negatively impact the user's productivity or interfere with work responsibilities;
- It is approved by the user's line management.

15. Exceptions

Certain situations may arise where an exception to this policy is warranted. Such exceptions must be requested in advance and approved in writing by the Cybersecurity Director and/or the ITSC.