Communications (Information Transfer) Security Management Policy

Objective and Scope

The objective of this document is to ensure the protection of transfer of information and other related processing facilities both internally and externally.

Roles, Responsibilities and Authorities

The Operations Director or competent IT Team delegate takes ownership of information transfer.

Where an exception or deviation from an expectation or plan occurs, the senior assigned role shall make the determination in terms of what is an acceptable change. The change management process may need to be enacted.

Legal and Regulatory

Title	Reference
Data Protection Act 2018	https://www.legislation.gov.uk/ukpga/2018/12/contents
General Data Protection Regulation (GDPR)	https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/
The Telecommunications (Lawful Business practice)(Interception of Communications) Regulations 2000	www.hmso.gov.uk/si/si2000/20002699.htm
Computer Misuse Act1990	www.hmso.gov.uk/acts/acts1990/Ukpga_19900018_en_1.htm
The Privacy and Electronic Communications (EC Directive) Regulations 2003	www.hmso.gov.uk/si/si2003/20032426.htm
The Freedom of Information Act 2000	https://www.legislation.gov.uk/ukpga/2018/12/contents
Online Safety Act 2023	https://www.legislation.gov.uk/ukpga/2023/50/contents/enacted
National Assistance Act 1948	https://www.legislation.gov.uk/ukpga/Geo6/11-12/29/enacted
Criminal Law Act 1967	https://www.legislation.gov.uk/ukpga/1967/58/introduction
The Copyright, Designs and Patents Act 1988	https://copyrightservice.co.uk/
Market Research Society Code of Conduct	https://www.mrs.org.uk/pdf/MRS-Code-of-Conduct-2019.pdf
Market Research Society Fair Data Principles	https://www.fairdata.org.uk/10-principles/

Communications (Information Transfer) Security Management Policy

ISO 27001/2 REFERENCES	ISO 27001: 2013 Clause ID	ISO 27002: 2013 Annex A ID	ISO 27001: 2022 Clause ID	ISO 27002: 2022 Control ID
Information transfer		13.2		5.14
Electronic messaging		13.2.3		5.14
Agreements on information transfer		13.2.2		5.14
Non-disclosure agreements / confidentiality		13.2.4		6.6

Related Information

- Non Disclosure Agreements
- Information Classification Policy
- Change Management Procedure
- IS Event Reporting Policy

Policy

The Operations Director determines and implements the rules and protocols for managing information transfer.

Security measures necessary for particular services, such as security features, service levels and service requirements, are implemented. Prevision Research ensures network service providers implement these measures.

Information transfer

Information is continually transferred both within the company and to various external entities by the following methods:

- General non-sensitive information may be shared via email, fax, voicemail, through meetings or other presentations such as slides or video. No electronic data attachments containing confidential or personal information can be sent other than via secure electronic media as approved by the Operations Director.
- Secure information transfer can be sent via secure electronic media accounts such as OneDrive, SFTP etc.

    1. *Microsoft OneDrive shall be used for operational files storage and transfer.*
    2. *Shared Drive allows secure handling, storage, malware, virus protection, backup and audit of files.*

Communications (Information Transfer) Security Management Policy

3. *Access is controlled and managed in accordance with the System and Application Access Control Policy.*
4. *Documents may be transferred between Prevision Research and clients with the use of shared folders in OneDrive.*
5. *Share folders [not high risk information/data content) must be shared to an individual client's known and authorised email address to manage secure access control.*
6. *High risk information/data content share folders must not be shared via email. This can only be transferred under agreement by the client / data recipient on written approval from the Operations Director under encryption to an equally secure folder on the client's drive - written approval from client received before transfer occurs.*

- Verbal transfer of information occurs through meetings, speaking at conferences, or presentations.

  Any discussions in meetings shall be documented and distributed to an agreed/approved list via electronic media.

  Conference presentations shall be approved by a designated manager prior to presentation. This approval checks for any CIA risk or PII release.

  Presentations (e.g. on YouTube) can only be developed and released after approval by a designated manager prior to presentation. This approval checks for any CIA risk or PII release.

Information transfer agreements

When information of a high risk nature is transferred electronically to external parties, agreements are set in place between both parties before data transfer occurs.

Agreements include the following to ensure transparency and clarity:

- individual responsibilities assigned to both sender and receiver for notification of sending and receipt of transmission
- minimum technical security standards for transmission and receipt
- access controls or parties agreed

Ensure traceability of transmission and receipt is maintained.

When physical media is transferred through courier services, the same principles of security apply with both parties agreeing on the courier service provider and any other third party involvement.

Electronic transfer of information

Electronic transfer includes email, electronic messaging, electronic data interchange or social networking are acceptable communications methods for general (not secure) information as long as the sender and credentials are known. The sending of business related messages from public websites is considered a risk.

When using electronic transfer the following principles apply:

- Devices providing electronic messaging provisions must be subject to 2FA to protect from unauthorised access, message modification or intrusion

Communications (Information Transfer) Security Management Policy

- Only send to known confirmed addresses associated with known individuals
- Do not send PII information or other classified information via text messaging

Sending information via physical storage transfer

This includes paper based information and data storage devices. Standards shall be followed to ensure:

- Traceability of transferred package from person sending to receiver
- Approved courier - receipt of pick up
- Appropriate waterproof protective packaging
- Receiver name and address
- Receipt of delivery

Receiving information via electronic transfer

When the need arises to receive a transfer of security or sensitive information to the company, request the sender to only transfer via a secure method.

Non-disclosure Agreements or other confidentiality agreements

Confidentiality Agreements (CA) and Non-Disclosure Agreements (NDA) are in place and required to be used in circumstances where access to personal information, business sensitive information or core software data is or may be accessible. Use the NDA for employees and CA for external parties.

NDA's and CAs will vary according to legislative jurisdictions.

- Signatories from both Prevision Research and the recipient must be in place. Prevision Research approval for authorisations is assigned to the Operations Director.
- NDAs and CAs must be dated and have a finite life 24 months before review and re-approval with a new NDA or CA as appropriate.
- Prescribed content and approved/agreed use of content as prescribed
- Right to audit and monitor compliance to the NDA and CA
- Document destruction arrangements

Policy review

This policy shall be reviewed by the policy owner annually or immediately after a process change or a policy breach is known to have occurred. Refer below for the most recent review.

History table

Date	Rev No	Changes	Reviewed By	Approved By	Training Y/N

Communications (Information Transfer) Security Management Policy
