Information and Data Security Policy

PFA Research Ltd

Contents

1 Policy Statement

PFA Research Ltd (PFA Research) takes its responsibility for information security very seriously. The company will protect the information entrusted to us by our clients, our strategic partners, research participants and other third party organisations by:

- Maintaining compliance with relevant UK and European Union legislation e.g. the Data Protection Act 2018 and the UK General Data Protection Regulation (UK GDPR);
- Ensuring effective policies and procedures are in place to support secure working practices;
- Educating and training our staff to handle and process information securely;
- Investigating and learning from all actual and suspected security incidents;
- Continuously reviewing and improving our information security arrangements.

All employees of PFA Research have a contractual responsibility to be aware of and conform to the company's values, rules, policies and procedures.

PFA Research commits to ensure the protection of all information assets within the custody of the Business. High standards of confidentiality, integrity and availability of information will be maintained at all times.

Overall responsibility for the policy's implementation lies with the managing director and the data protection officer.

2 Purpose

Information is a major asset that PFA Research has a responsibility and requirement to protect.

Protecting information assets is not simply limited to covering the stocks of information (electronic data or paper records) that PFA Research maintains. It also addresses the people that use them, the processes they follow and the physical computer equipment used to access them.

This Information Security Policy addresses all these areas to ensure that high confidentiality, quality and availability standards of information are maintained.

The following policy details the basic requirements and responsibilities for the proper management of information assets at PFA Research Ltd. The policy specifies the means of information handling and transfer within the company.

3 Scope

This Information Security Policy applies to all the systems, people and business processes that make up the company's information systems. This includes all executives, partners, employees, contractual third parties and agents of PFA Research who have access to information systems or information used for carrying out the work of PFA Research.

4 Definition

This policy and standard operating procedure (SOP) should be applied whenever business information systems or information is used. Information can take many forms and includes, but is not limited to, the following:

- Hard copy data printed or written on paper

- Data stored electronically
- Communications sent by post/courier or using electronic means
- Stored tape or video
- Recorded speech

5 Risks

PFA Research recognises that there are risks associated with users accessing and handling information in order to conduct official business.

This policy aims to mitigate the following risks:

- Misunderstandings or lack of awareness of what constitutes information
- Non-reporting of information security incidents
- Inadequate destruction of data
- Loss of direct control of user access to information systems and facilities

Non-compliance with this policy could have a significant effect on the efficient operation of the organisation and may result in financial loss and an inability to provide necessary services to our customers.

6 Key Messages

- The company must draw up and maintain inventories of all important information assets.
- All information assets, where appropriate, must be assessed and classified by the owner in terms of sensitivity and which staff/contractors require access.
- Access to information assets, systems and services must be conditional on acceptance of the appropriate acceptable usage policy.
- Users should not be allowed to access information until the line manager, operations manager and/or manging director is satisfied that they understand and agree the legislated responsibilities for the information that they will be handling.
- Restricted access information must not be disclosed to any other person or organisation via any insecure methods including, but not limited to, paper-based methods, fax, telephone (especially if calls are recorded) or electronic mail.
- Disclosing information that has restricted classification or otherwise is client confidential to any external unauthorised organisation is prohibited and is a disciplinary offence.
- Any client and project related data shared shall be transferred via PFA Research's Microsoft 365 environment. Please see data sharing procedure.
- Any client and project related data can not be emailed and/or shared via personal accounts, including but not limited to, personal emails, social media accounts, communications platforms, etc.
- All client and project related material, including but not limited to data, communications must be stored and transferred only within the PFA Research Microsoft 365 environment. Exception can be made if the client needs/request overwrites this principle.

7 Information asset assessment

Classification	Description	Examples	Risk Rating / Impact	Security controls
Protected	Sensitive personal data, including data that through disclosure would lead to substantially prejudice the interests of any person and/or organisation and would be actionable by another party.	A person's medical information. Disciplinary records. Information on persons under age.	High – Disclosure of personal data would constitute a breach of the UK GDPR, Data Protection Act and would be actioned by the ICO, including possible fines. Risk to the individual and the company and clients.	Data transfer only if absolutely necessary and only via secure and encrypted data transfer portals. Restricted access network areas (permission depending drives and/or folders as necessary).. Access to data on a 'need to know' basis only. Management access to SharePoint only via dedicated hardware (company provide laptops) using two factor verification. Hard copies are to be stored in locked cabinets only. No records to remain on desks unattended.
Confidential	Any personal and confidential information, including data that through disclosure would prejudice the interests of any person and/or organisation.	Staff records. Survey respondents information. Client confidential information. Client commercially confidential information.	High – Disclosure of personal data would constitute a breach of the UK GDPR, Data Protection Act and would be actioned by the ICO, including possible fines. Risk to the individual and the company and clients.	Data transfer only if necessary and only via secure and encrypted data transfer portals. Restricted access network areas (permission depending drives and/or folders as necessary).. Access to data on a 'need to know' basis only. Management access to SharePoint only via dedicated hardware (company provide laptops) using two factor verification. Hard copies are to be stored in locked cabinets only. No records to remain on desks unattended.

Internal	General information circulated within the company in regard to the running of projects and the business that does not include personal, personal sensitive, commercially confidential or client confidential data.	Staff communications to hours of work offered. Project progress and management (not including personal, personal sensitive or other confidential material). General business communications.	Medium – Minimal or no risk to individuals, potential risk to company's integrity.	Electronic server-stored data whenever possible. For data shared through internal emails, use of referential links to information rather than attached documents.
Public	Information available in the public domain.	Information provided by other bodies and needed in reference to the company's work. For example, data provided by the Office of National Statistics.	Low – no personal data is collected or stored. No risk to individuals.	None required, however, sharing and distribution of information should only happen if necessary.

9 Access control

PFA Research controls access to data and information assets through the following:

- Dedicated, licensed Microsoft SharePoint account (MS365) for any data entrusted to us, no storage of any client data (i.e. data entrusted to us or collected on behalf of) in any other cloud environment (with the exception of call recordings being stored via dedicated VoIP software portal 3CX or where data sub-processing agreements are in place with SaaS) or on individual laptop or PCs.
- All data is held behind firewalls.
- Only senior members of staff are able to download any content onto PFA Research's IT equipment in order to minimize the introduction of any malicious software into our systems. These measures secure our data and data held by us against cybercrime.
- Our locations in facilitated office buildings ensures data is protected from conventional crime by a number of security measures, including a key-card and alarm secured designated office, key-card secured building sections, and an overall intruder alarm for the buildings. There are also CCTV cameras in operation.
- MS365 SharePoint assured data back-ups ensure business continuity and prevent the loss of data for disaster recovery.
- Additional data back up is undertaken via Redstor to ensure business continuity and prevent the loss of data for disaster recovery.
- A structured and organised electronic filing system is used to ensure secure and separate file retention amongst all client projects and/or PFA Research company files.
- Each client project is assigned a unique project reference (UPR) for easy and speedy identification. Each document carries this UPR. Client projects are assigned a dedicated space on the company's drive adhering to a defined folder structure.
- Access privileges to client and project documentation are granted on a need to know/work basis only.
- All company devices are connected to Azure AD and set up with multifactor authentication. Passwords, pin and biometrics/Windows Hello for Business is used on all devices, with a pin being a minimum of 6 characters and mobile devices use pin code and/or biometrics including fingerprint scanner. All user accounts, are protected by user name, password and multifactor authentication. Individual user accounts can be disabled from the main administration site on MS365 SharePoint.
- The majority of equipment has no capacity to upload or download data via data storage devices such as USB sticks or CD rom. Only management has permission to down and upload data via data storage devices such as USB sticks or CD rom.
- User names are issued by PFA Research and passwords are set by individual users.
- Access to written or printed materials as well as access to computer systems (i.e. physical and logical access) are reviewed permanently. Each client project is assessed in order to understand which members of staff needs full access to all materials and which employees need restricted or limited access to selected materials in order to undertake their work.

- Written or printed materials are stored securely, if and when the needs arise, for security and in order to limit access.
- Access to electronic data is granted via individual user accounts only and those accounts are disabled during lengthy absence by the member of staff or when leaving the employment.

10 Policy Compliance

This policy is part of the PFA Research employee handbook and staff are made aware of this policy. Complying with the policy and the associated procedures is a key requirement. The policy is also published on the PFA Research website (www.pfa-research.com/gdpr) and via the employee portal.

Staff are encouraged to feedback any suggestions or concerns they have on any or all aspects of compliance, this or other policies or procedures.

If any user is found to have breached this policy, they may be subject to PFA Research's disciplinary procedure. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

If you do not understand the implications of this policy or how it may apply to you, seek advice from your line manager, the data protection officer or managing director.

11 References

The following PFA Research policy documents are directly relevant to this policy, and are referenced within this document:

- UK General Data Protection Regulation (UK GDPR) Policy
- Data Protection Policy
- Email and Internet Policy
- Business Continuity Management Plan
- Emergency Response Plan

12 Authorisation, Approval and Review Dates

This Policy will be subject to review annually. This review will not preclude any amends to this or other policies in the interim, should they be deemed necessary or required by law.

Any questions and enquiries in relation to this policy and the associated procedures should be addressed to the line manager, data protection officer or managing director.

13 Alternative Formats

PFA Research . Would like to ensure that your needs are met. If you need this information in any other format or translated into a language other than English, please contact:

PFA Research Ltd
Tremough Innovation Centre
Penryn
Cornwall
TR10 9TA
Tel: 01326 375705
info@pfa-research.com

www.pfa-research.com

14 Version History

Reviewed	Next Review	Reviewed by
October 2017	March 2018	Beate Galke – Project Manager.
May 2018	May 2019	Beate Galke – Operations Manager
May 2019	May 2020	Beate Galke – Operations Manager
August 2020	August 2021	Beate Galke – Operations Manager
November 2020	January 2021	Beate Galke – Operations Manager – Policy reviewed early with EU Exit in mind. Currently no clear guidelines available from UK Government. Policy to be reviewed if and when finalised guidelines become available, but no later than January 2021.
January 2021	November 2021	Beate Galke – Operations Manager – No further guidelines available, review later this year, but no later than November 2021.
October 2021	October 2022	Beate Galke – Operations Manager
May 2022	May 2023	Beate Galke – Operations Manager Review following change over to MS365 Sharepoint
October 2022	October 2023	Beate Galke – Operations Manager Included key messages around data sharing and information storing 'Key messages' Next review to be undertaken when folder structure is changed.
May 2024	May 2025	Beate Galke – Operations Manager Policy has been under review since March 2023 to allow for changes in PFA

		Research's implementation and use of SaaS providers. Since gaining Cyber Essential certification in 2023, this policy has now been updated in line with new working procedures.