Challenge-trg Group Ltd Information Security Policy

Foreword

In the current “digital age” we have seen tremendous change in the way we generate, store and exchange information. It has also profoundly altered the terms by which we interact with each other, not just as individuals, but also within and between organisations, our clients and employees.

We have gained great benefits from this “digital age”, but it brings with it profound challenges in the areas of security and privacy, which have been reflected in legislative changes within the European Union concerning the holding of information.

As a leading employment business committed to service delivery and innovation, Challenge-trg Group has an ethical, legal and professional duty to ensure that the information it holds conforms to the principles of confidentiality, integrity and availability.

We must ensure that the information we hold or are responsible for is safeguarded where necessary against inappropriate disclosure; is accurate, timely and attributable; and is available to those who should be able to access it, as a minimum standard ensuring it conforms to the data principles set out with the Data Protection Act (DPA) and the General Data Protection Regulations (GDPR).

The Information Security Policy below provides the framework by which we take account of these principles. Its primary purpose is to enable all Challenge-trg Group staff and employees/contractors to understand both their legal and ethical responsibilities concerning information, and empower them to collect, use, store and distribute it in appropriate ways.

This policy is the cornerstone of Challenge-trg Group’s on-going commitment to enhance and clarify our information security procedures. It has my full support and I encourage all Challenge-trg Group staff and employees/contractors to read it and abide by it in the course of their work.

James Davies
Group Director of HR

Challenge-trg Group

1. INTRODUCTION

The confidentiality, integrity and availability of information, in all its forms, are critical to the on-going functioning and good governance of Challenge-trg Group. Failure to adequately secure information increases the risk of financial and reputational losses from which it may be difficult for Challenge-trg Group to recover.

This information security policy outlines Challenge-trg Group's approach to information security management. It provides the guiding principles and responsibilities necessary to safeguard the security of the organisations information systems. Supporting policies, codes of practice, procedures and guidelines provide further details.

Challenge-trg Group is committed to a robust implementation of Information Security Management. It aims to ensure the appropriate confidentiality, integrity and availability of its data. The principles defined in this policy will be applied to all of the physical and electronic information assets for which Challenge-trg Group is responsible.

Challenge-trg Group is specifically committed to preserving the confidentiality, integrity and availability of documentation and data supplied by, generated by and held on behalf of third parties pursuant to the carrying out of work agreed by contract in accordance with the requirements of GDPR, the 7 Data Protection Principles of DPA and the 10 Steps to Cyber Security issued by the National Cyber Security Centre.

1.1 OBJECTIVES

The objectives of this policy are to:

1. Provide a framework for establishing suitable levels of information security for all Challenge-trg Group information systems (including but not limited to our personal Cloud environments run by Challenge-trg Group, computers, storage, mobile devices, networking equipment, software and data) and to mitigate the risks associated with the theft, loss, misuse, damage or abuse of these systems. This explicitly includes:
    a) The resources required to manage such systems will be made available
    b) Continuous improvement of any ISMS/portal will be undertaken

2. Make certain that users are aware of and comply with all current and relevant UK and EU legislation as detailed above.

3. Provide the principles by which a safe and secure information systems working environment can be established for staff, employees/contractors and any other authorised users.

4. Ensure that all users understand their own responsibilities for protecting the confidentiality and integrity of the data that they handle.

5. Protect Challenge-trg Group from liability or damage through the misuse of its IT facilities.

6. Maintain research data and other confidential information provided by suppliers at a level of security commensurate with its classification, including upholding any legal and contractual requirements around information security.

7. Respond to changes in the context of the organisation as appropriate, initiating a cycle of continuous improvement.

1.2 SCOPE

This policy is applicable to, and will be communicated to, all staff, made available to view on our company intranet/website and third parties who interact with information held by Challenge-trg Group and the information systems used to store and process it.

This includes, but is not limited to: Cloud systems developed or commissioned by Challenge-trg Group, any systems or data attached to the Challenge-trg Group data or telephone networks, systems managed by Challenge-trg Group or its IT Service Provider, mobile devices used to connect to Challenge-trg Group networks or hold Challenge-trg Group data, data over which Challenge-trg Group holds the intellectual property rights, data over which Challenge-trg Group is the data controller or data processor, electronic communications sent from Challenge-trg Group.

2. POLICY

2.1 Information Security principles

The following information security principles provide overarching governance for the security and management of information at Challenge-trg Group.

1. Information should be classified according to an appropriate level of confidentiality; integrity and availability (see Section 2.3. Information Classification) and in accordance with relevant legislative, regulatory and contractual requirements (see Section 2.2. Legal and Regulatory Obligations).

2. Staff with particular responsibilities for information (see Section 3. Responsibilities) must ensure the classification of that information; must handle that information in accordance with its classification level; and must abide by any contractual requirements, policies, procedures or systems for meeting those responsibilities.

3. All users covered by the scope of this policy (see Section 1.2. Scope) must handle information appropriately and in accordance with its classification level.

4. Information should be both secure and available to those with a legitimate need for access in accordance with its classification level:

    a. On this basis, access to information will be on the basis of least privilege and need to know.

5. Information will be protected against unauthorized access and processing in accordance with its classification level.

6. Breaches of this policy must be reported (see Sections 2.4. Compliance and 2.5. Incident Handling).

7. Information security provision and the policies that guide it will be regularly reviewed, including through the use of annual internal audits and penetration testing.

8. Any explicit Information Security Management Systems (ISMSs) run by Challenge-trg Group will be appraised and adjusted through the principles of continuous improvement.

9. All Challenge-trg Group DSE users will operate a clean Desk/Screen policy, only have information in front of you that you are actively working on, when finished, the information should

be locked securely away, if you need to step away from your computer screen, all users must lock their work station to prevent unauthorised access to our network and information. While on lunch and at the end of the working day, you must clear your desk of any information that would be considered private and confidential or business sensitive. During lunch, you must lock your workstation and at the end of the day, you must log out of your session.

2.2 Legal and Regulatory Obligations

Challenge-trg Group has a responsibility to abide by and adhere to all current UK and EU legislation as well as a variety of regulatory and contractual requirements.

A non-exhaustive summary of the legislation and regulatory and contractual obligations that contribute to the form and content of this policy is provided in Appendix A.

Related policies will detail other applicable legislative requirements or provide further detail on the obligations arising from the legislation summarised below

2.3 Information Classification

The following table provides a summary of the information classification levels that have been adopted by Challenge-trg Group and which underpin the 8 principles of information security defined in this policy.

These classification levels explicitly incorporate the General Data Protection Regulation's definitions of Personal Data and Special Categories of Personal Data, as laid out in Challenge-trg Group's Data Protection Policy,
and are designed to cover both primary and secondary research data.

Information may change classification levels over its lifetime, or due to its volume – for instance:

- An individual such as a driver may work over many locations and may be managed by more than one Manager who will have access to that individuals personal data e.g. Driving License, CPC Card information.

Security Level	Definition	Examples
1. Confidential	Normally accessible only to specified members of Challenge-trg Group staff. Stored within a restricted area	GDPR-defined Special Categories of personal data (racial/ethnic origin, political opinion, religious beliefs, trade union membership, physical/mental health condition, Passwords
2. Restricted	Normally accessible only to specified members of Challenge-trg Group staff. Stored within a restricted area Clients will process this information for compliance/entitlement to undertake role. E.g. Driving License checks at assessment.	GDPR-defined Personal Data (information that identifies living individuals including home / work address, age, telephone number, photographs); draft reports, papers and minutes; systems;
3. Internal use	Normally accessible only to specified	Internal correspondence, always

	members of Challenge-trg Group staff. Stored within a restricted area for emails	communicated via Challenge-trg Group systems e.g. email or phone. Internal reports e.g. Weekly Update (HR 44)
4. External use	Normally accessible only to the intended parties e.g. Commercially Confidential Documents	Performance reports to clients, any third party that has a business dealing (or potential)
5. Public	Published Accounts, Any information on our website or social media accounts	Year end accounts, social media posts, linkedin. Job Boards

2.4 Suppliers/Clients

All Challenge-trg Group's suppliers/clients will abide by Challenge-trg Group's Information Security Policy, or otherwise be able to demonstrate corporate security policies providing equivalent assurance. This includes:

- when accessing or processing Challenge-trg Group data, whether on site or remotely
- when subcontracting to other suppliers.

2.5 Cloud Services

Challenge-trg Group operates its own Personal Cloud which is hosted on its own servers held in a Tier 3 Data Centre within the UK, from time to time, for the better performance of its cloud systems, third parties will require restricted access in order to undertake maintenance of their specific programmes operating within our cloud, these are:

- RSM to maintain our payroll software (INPAY) Restricted Access
- Access Dimensions (Credit Control/Finance system) Restricted Access
- Trunk Networks – IT Support Company who looks after the day to day maintenance of our IT – Full Access in so far that it relates to support.

Challenge-trg Group operates a remote desktop environment (Citrix) which prevents data being transferred to local devices e.g USB storage stick or the laptop's internal storage disk.

2.6 Compliance, Policy awareness and Disciplinary procedures

Any security breach of Challenge-trg Group's information systems could lead to the possible loss of confidentiality, integrity and availability of personal or other confidential data stored on these information systems.

The loss or breach of confidentiality of personal data is an infringement of the General Data Protection Regulation, contravenes Challenge-trg Group's Data Protection Policy, and may result in criminal or civil action against Challenge-trg Group.

The loss or breach of confidentiality of contractually assured information may result in the loss of business, financial penalties or criminal or civil action against Challenge-trg Group. Therefore it is crucial that all users of Challenge-trg Group's information systems adhere to the Information Security Policy and its supporting policies as well as the Information Classification Standards.

All current staff and other authorised users will be informed of the existence of this policy and the availability of supporting policies, codes of practice and guidelines. Any security breach will be handled in accordance with all relevant Challenge-trg Group policies, including Laptop, Mobile and the appropriate disciplinary policies.

2.7 Incident Handling

Breaches of personal data will be reported to the Information Commissioner's Office within 72 hours of a confirmed breach by Challenge-trg Group's Commercial Director or Group Director of HR in their absence. If necessary, staff of Challenge-trg Group can also use Challenge-trg Group's Whistle Blowing Policy (Public Interest Disclosure) which can be found on its website (www.challengetrg.co.uk) within the policies section.

Where a Client's data has been breached, we will notify them within 12 hours of the confirmed breach.

Alternatively you can report a breach to the Commercial Director on 0208 971 1900 or in their absence the Group Director of HR on 0208 971 1900 selecting option 3

For potential breaches, please direct these to the Commercial Director or in their absence, the Group Director of HR using the contact information above.

2.8 Supporting Policies, Codes of Practice, Procedures and Guidelines

Supporting policies have been developed to strengthen and reinforce this policy statement. These, along with associated codes of practice, procedures and guidelines are published together and are available on Challenge-trg Group's website. Such policies include:

- HR06 Data Protection Policy
- HR27 Social Media Policy
- HR45 Company Employee Laptop Policy
- HR58 Company Mobile Phone Policy
- HR64 ISMS Data Transfer Policy and procedures

All staff and any third parties authorised to access Challenge-trg Group's network or data are required to familiarise themselves with these supporting documents and to adhere to them in the working environment.

2.9 Review and Development

This Policy and its subsidiaries will be reviewed by the Challenge-trg Group board and Senior Management in collaboration with its IT Support Partner.

Any reviews undertaken will be documented within Challenge-trg Group's ISO9001:2015 Quality Management System.

3.0 Responsibilities

All members of Challenge-trg Group, agency staff/Contractors working with Challenge-trg Group, third parties and collaborators on Challenge-trg Group projects may be users of Challenge-trg

Group information. This carries with it the responsibility to abide by this policy and its principles and relevant legislation, supporting policies, procedures and guidance.

No individual should be able to access information to which they do not have a legitimate access right. Notwithstanding systems in place to prevent this, no individual should knowingly contravene this policy, nor allow others to do so. To report policy contraventions, please see *Section 2.5: Incident Handling.*

Many members of Challenge-trg Group have specific responsibilities relating to specific data, they are:

CEO – unrestricted access to financial, CMS Reporting
MD – unrestricted access to financial, CMS
Commercial Director – unrestricted access to all areas (IT Admin)
Regional Managers – CMS including default reports
Group Director of HR – CMS Full access to all personnel details including salaried staff
Senior Contract Managers - CMS Full access to their respective sites including default reports
Contract Managers – CMS Full access to their respective site
Hub Managers – CMS Full access to their respective site
Senior Recruitment Consultants - CMS Full access to their respective site
Recruitment Consultants - CMS Full access to their respective site
Consultants - CMS Full access to their respective site
Administrators - CMS Full access to their respective site

As previously defined, Challenge-trg Group operated a personal cloud with the following drives:

(For the purposes of security, the drive letters do not accurately reflect the actual drive names)

A:/ This drive holds shared information and forms part of its intranet where staff can access relevant forms and procedures. There are various folders which have restricted access relevant to the parties that need to access that specific folder.
B:/ This drive holds financial information and is restricted to those only working within the fiancé department.

C:/ Is a person's home drive, no one else has access to this drive (save for IT Administrators)

D:/ Is the fax/scan drive – all information in this area will be cleansed every 24 hours.

E:/ Is the HR folder contained in one of the areas, the only persons who have access to this drive are:

- Managing Director
- Commercial Director (IT Admin only)
- Group Director of HR
- Other HR staff

Our IT Support Service (Trunk Networks) has access to all of the above, only for the purpose of undertaking IT Administrative duties and are aware that access is only given when any member of Staff require their help. Protocols are in place that requires the authorisation of the Group Director of HR before certain IT Administrative duties are undertaken e.g. giving access to another person's area for legitimate business reasons.

3.1 Authorisation levels

In Line with the Responsibilities section, the following Authorisation levels have been assigned in accordance with ISO 27001 s.2.2.

Job Title	Authorisation level	Authorisation Information
CEO/MD	1-5	1-5
Commercial Director	1-5	1-5
Group Director of HR	1-5	1-5
Regional Managers	3-5	1-5 in their region
Contract/Hub Managers	3-5	1-5 on their site
Senior Recruitment Consultants	3-5	3-5 on their site
Finance Staff	3-5	3-5
Admin/operational Staff	3-5	3-5 on their site

4.0 Appendix A – A summary of relevant information

4.1 Computer Misuse Act 1990

Defines offences in relation to the misuse of computers as:

1. Unauthorised access to computer material.
2. Unauthorised access with intent to commit or facilitate commission of further offences.
3. Unauthorised modification of computer material.

4.2 Defamation Act 1996

“Defamation is a false accusation of an offence or a malicious misrepresentation of someone's words or actions. The defamation laws exist to protect a person or an organisation's reputation from harm.”

4.3 Obscene Publications Act 1959 and 1964

The law makes it an offence to publish, whether for gain or not, any content whose effect will tend to "deprave and corrupt" those likely to read, see or hear the matter contained or embodied in it. This could include images of extreme sexual activity such as bestiality, necrophilia, rape or torture.

4.4 Protection of Children Act 1978, Criminal Justice Act 1988, Criminal Justice and Immigration Act 2008.

The Protection of Children Act 1978 prevents the exploitation of children by making indecent photographs of them and penalises the distribution and showing of such indecent photographs. Organisations must take appropriate steps to prevent such illegal activities by their workers using their digital systems and networks.
The definition of ‘photographs’ include data stored on a computer disc or by other electronic means which is capable of conversion into an image.

It is an offence for a person to […] distribute or show such indecent photographs; or to possess such indecent photographs, with a view to their being distributed or shown by himself or others.

Section 160 of the Criminal Justice Act 1988 made the simple possession of indecent photographs of children an offence. Making an indecent image of a child is a serious arrestable offence carrying a maximum sentence of 10 years imprisonment. Note: The term "make" includes downloading images from the Internet and storing or printing them out.

4.5 Terrorism Act 2006

The TerrorismAct2006 makes it an offence to write, publish or circulate any material that could be seen by any one or more of the persons to whom it has or may become available, as a direct or indirect encouragement or other inducement to the commission, preparation or instigation of acts of terrorism. It also prohibits the writing, publication or circulation of information which is likely to be useful to anyone or more persons in the commission or preparation of terrorist acts or is in a form or context in which it is likely to be understood by anyone or more of those persons as being wholly or mainly for the purpose of being so useful.

In addition, it prohibits the glorification of the commission or preparation (whether in the past, in the future or generally) of terrorist acts or such offences; and the suggestion that what is being glorified is being glorified as conduct that should be emulated in existing circumstances.

4.6 General Data Protection Regulation

The GDPR will apply in the UK from 25 May 2018.The government has confirmed that the UK's decision to leave the EU will not affect implementation of the GDPR. The GDPR reinforces and extends data subjects' rights as laid out in the Data Protection Act(1998), and provides additional stipulations around accountability and governance, breach notification and transfer of data. It also extends the maximum penalties liable due to a data breach, from £500,000 to 4% global turnover.

The GDPR requires Challenge-trg Group to maintain an Information Asset Register, to ensure where personal data is voluntarily gathered people are required to explicitly opt in, and can also easily opt out. It requires data breaches to be reported to the Information Commissioner's Office within 72hrs of Challenge-trg Group becoming aware of their existence.