Perform Green
Information and Data Security Policy

Table of Contents

DOCUMENT INFORMATION

Author: C Hewitt
Owner: B Smith

VERSION HISTORY

Amendment/Reason	Version	Date
Created	1.0	September 2016
Amended	1.1	January 2017
Update following annual re-accreditation	1.2	January 2018
New Template & review	1.3	July 2018
Review	1.4	July 2019
Review	1.5	August 2020
Template update	2.0	February 2021
Information update	2.1	March 2021
Information update	3	December 2021

Introduction

Effective information and data security is a key priority for Perform Green, and cyber security threats continue to become more prevalent. It is vital for client confidence and for the efficient, effective and safe conduct of Perform Green's business. In carrying out its business Perform Green obtains, processes and manages information from individuals and organisations which must be managed appropriately and securely.

Perform Green recognises that stringent principles of information and data security must be applied to all information it holds.

Perform Green is committed to ensuring that all the information held is managed lawfully and appropriately. Legislation including The Data Protection Act 1998, Freedom of Information Act 2000 and Computer Misuse Act 1990 set the legal framework within which Perform Green must operate and ensure the safe storage and handling of information. Perform Green fully appreciates and will take the necessary actions to ensure that it continues to comply with all legislation regarding its management of personal data and other information.

Perform Green fully accepts the need for accountability and explicit assurance that we will continue to maintain high standards of data security. This responsibility is not limited just to Perform Green, but equally applies to its delivery partners, contractors, suppliers and any other third party organisation/person contracted to support Perform Green in its delivery of services to clients.

We are registered with the Information Commissioner to store and process data; furthermore, we have accreditation under the Cyber Essential Scheme and Information Assurance for SME's Information Security Standard, and will continue to maintain it.

Perform Green complies with the requirements of the Cyber Essentials Scheme Our certificate of assurance number is: IASME-CE-032551

Perform Green complies with the IASME Information Security Standard Our certificate of assurance number is: IASME-SA-001446

Perform Green is registered to store and process data. Our Data Protection Registration is: ZA209253

Policy Statement

- Perform Green regards the lawful and correct treatment of information and data as essential to its successful operations and to maintaining the confidence and trust of clients and those with whom it conducts business.
- Perform Green fully endorses and adheres to the eight principles of Data Protection as laid out in the Data Protection Act (See Appendix 1). In particular principle seven, which deals with security states:

“Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data."

- Perform Green seeks to foster a culture that values, protects and uses information for the good of our business and that of our client organisations through a range of data security methods and arrangements set out below.
- We are committed to assuring and demonstrating our commitment to information security by achieving and sustaining appropriate accreditations to give us, our clients and our partners’ confidence that any information or data shared with us is safe in our hands.

Policy in Action

Ownership and Confidentiality

All personal data is maintained for the purpose defined within the notification under the Data Protection Act. The Data Owner is responsible for maintaining the data protection notification, dealing with subject access requests, maintaining awareness of Data Protection legislation and data security policy and practices. A record of catagories and purpose will be maintained by the Data Owner, including whether we are Data Controller or Data Processor.

Governance and Accountability

Effective governance and accountability arrangements are essential to ensure the proper management and control of information. All Perform Green Directors, Staff and Partners are made aware of their responsibilities for information and data security to maintain data security and confidentiality at all times (see Appendix 2: Data Security Agreement). The following paragraphs detail the oversight roles and responsibilities that Perform Green has in place to deliver an effective data governance regime.

We will undergo at least annual reviews of our policies, processes and systems to ensure – seeking independent accreditation to give us assurance that we are meeting our own standards.

Information and Data Security Director / Data Owner / SIRO

Barney Smith, Founder and CEO at Perform Green Ltd, is the Senior Information Risk Owner.

Clare Hewitt, Deputy CEO, is the Information Data Security Officer and *Data Owner* and has ultimate responsibility for information and data security within Perform Green. This role encompasses ensuring Perform Green fulfils its data governance responsibilities and risk management processes. The Data Owner is responsible for specifying the standards of data security that apply to each Client project.

Project Leaders / Account Managers

Individual project leaders or Account Managers in Perform Green are responsible for the secure management of information within their projects and team. They are also the primary liaison contact point on data security matters, including performance reporting; incident reporting; raising information security awareness, and audit and accountability matters.

All Staff and Partners

All Staff and Partners have a personal responsibility to safeguard the integrity and confidentiality of Perform Green's systems, data and physical facilities.

Managers (Project leaders, Directors etc.) are responsible for the application of the data security policy for matters under their control. They must ensure that all staff are aware and comply with the policy, which will be reflected in employment contracts.

Users of Perform Green systems are responsible for ensuring that data and information to which they have authorised access is used only for the purpose provided and that the confidentiality and integrity of the data is maintained. Associates will sign up to security policies through Associate Contracts.

Data Access and Disposal

Our systems are secured with, at minimum, 2 Factor Authentication, EU-US Privacy Shield Framework, SOC Type II Level 2 accreditation and encryption at rest and in transit. Access to each data store is limited to those needing such access to do their job. Each member of staff with such data access is personally responsible for maintaining the confidentiality of the data to which he/she has access.

The Data Owner determines who should have access to data and the retention requirements. If data is to be deliberately destroyed, then the Data Owner or their agent (whether internal or externally contracted) must ensure that destruction takes place in conditions compliant with the Data Protection Act.

Physical Security

Information and Data, whether in electronic or physical form, is subject to physical security control appropriate to its nature. All personal computers and data storage devices must be kept in securely locked buildings. Laptops and other portable data storage devices must not be left unattended when away from secure offices and must be at minimum password protected. All laptops have hard drives encrypted, and all devices are password and/or PIN protected.

Electronic Storage Systems

Data may be held on cloud-based servers and mobile devices such as laptops which will at minimum be encrypted at rest and in transit. We do not allow anyone to maintain our information on removable media such as USB sticks and readable CD's/DVD's. Information passed to us in this form will be transferred to other storage systems and wiped or otherwise destroyed.

Data held on cloud-based servers are the responsibility of the Perform Green Data Security Officer, who will be responsible for the security of data deposited on these servers.
Security of data held on personal computers and portable devices is the responsibility of the individual member of staff or associate who operates the equipment.

We have implemented encryption on our hardware and cloud systems & enabled firewalls.

Electronic Communication Systems

General data communication facilities such as e-mail and online conferencing are provided for business purposes and the data generated by these is treated as belonging to the organisation.

We require up to date anti-malware, firewalls and supported Operating Systems at minimum, with regular security patches installed at minimum.

We require complex passwords when using cloud-based services of at least 8 characters, such as email, as well as 2 Factor Authentication. When transmitting personal data and in particular data about others through such general facilities users must:

- abide by Perform Green data security protocols
- be aware that the constraints of the Data Protection Act and GDPR apply
- be aware that such transmissions are not secure and may be viewed by third parties and
- be aware of the possibility of both disciplinary procedures for misuse and/or legal proceedings with regard to, inter-alia, defamation, copyright and data protection.

Data Back Up, Business Continuity and Disaster Recovery

We will have a Business Continuity and Disaster Recovery Plan. As part of this, backup copies of programmes and data appropriate to the requirements of the business will be kept as determined by the Data Owner, organisational and legal requirements. This will include backups on and off site.

Protective Marking

We work with a number of public bodies, and along with other clients, they will have their own security policies. We will review the applicability of their policies for our engagements and apply them, in particular Government Security Classifications where we are likely to work with ‘Official’ and ‘Official-Sensitive’ materials.

Appendix 1: The Eight Data Protection Act Principles

The act contains eight “Data Protection Principles”.

These specify that personal data must be:

- Processed fairly and lawfully.
- Obtained for specified and lawful purposes.
- Adequate, relevant and not excessive.
- Accurate and up to date.
- Not kept any longer than necessary.
- Processed in accordance with the “data subject’s” (the individual’s) rights.
- Securely stored and processed.
- Not transferred to any other country without adequate protection in situ.

Appendix 2: Data Security Agreement

All Perform Green partners and staff are required to follow a data security agreement as set out below, this will form part of Employment and Associate Agreements:

To: [name]

Perform Green LTD (PG) will provided you with access to online and offline databases containing confidential information about clients, suppliers and other members of the PG staff. If you use your own equipment, it must be secure, have appropriate up to date anti-malware software operating and be using a supported Operating System. Hard-drives must be encrypted.

It is our duty under the terms of our Data Protection registration to take all reasonable steps to ensure that the information held on our database is used only for the purpose for which it was intended, and that access to this information is only made available to those who have a legitimate business purpose for seeing it.

By signing this agreement, you undertake to respect the confidentiality of the information held by PG, and to make use of this information solely in connection with your work with PG. You further undertake to take all reasonable steps to ensure that physical or electronic access to PG's data is restricted to you only, and that you will not share or in any other way pass on your security details to any third party.

Where you are required to have access to client data, you must ensure that access to such data is restricted to you alone, unless express permission from PG Chief Operating Officer, Director or the client is granted.

Any PG or client data stored on computers or other portable storage devices you control must be password protected, backed up, and must not be left unattended outside of secure PG, Client or Staff premises. USB storage must not be used for PG data.

If you become aware that your username and password or other security details have been obtained by any third party, you must inform a partner of PG immediately, so that the passwords can be reset.

Clare Hewitt, Deputy CEO, Perform Green LTD

Signed _____ Date _____

I agree to respect the confidentiality of Perform Green and Client data, and to take all reasonable steps to maintain the security of the data, as outlined above.

Signed _____ Date _____

Name _____ _____

Perform Green: Creating a Green and Smart Society

www.performgreen.co.uk