PALACE FOR LIFE FOUNDATION

POLICY TITLE:	DATA PROTECTION & PRIVACY FRAMEWORK
EFFECTIVE DATE:	1ST JULY 2018
WITHDRAWAL / RENEWAL DATE:	30TH JUNE 2019
QUERIES:	DUNCAN ROBINSON (HR)
LENGTH OF DOCUMENT:	22 PAGES

TABLE OF CONTENTS

DATA PROTECTION POLICY

The General Data Protection Regulation (GDPR) lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data and protects fundamental rights and freedoms of natural persons, in particular their right to the protection of personal data. The Act came into force on the 25th May 2018.

The Act is overseen and enforced by the Information Commissioners Office (ICO), who is an independent public body responsible directly to Parliament.

The two principal focuses of our policy relate to: i) Data collected about Foundation Staff and ii) Data collected relating to participants who are engaged in Foundation activities, programmes or football courses.

The Palace for Life Foundation, as a data controller, will be open and transparent when processing and using personal information by following the below 2 principles:

1. Personal data shall be:

   a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');

   b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');

   c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

   d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

   e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');

   f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss,

destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

1. Scope of Policy

This policy applies to all members of Palace for Life Foundation. For the purposes of this policy, the term 'staff' means all members of the Foundation staff including permanent, fixed term and temporary staff, Trustees, secondees and any third party representatives engaged or acting on behalf of the Foundation.

2. Definitions

2.1 This policy applies to all personal and sensitive personal data processed and stored electronically (1) and manually (paper based) files (2). It aims to protect and promote the rights of individuals ("Data Subjects") and the Foundation.

i) This list is not exhaustive: PCs, Laptops, Tablets, Phones.

ii) Manual records are paper based and structured, accessible and form part of a relevant filing system (filed by subject, reference, dividers or content), where individuals can be identified and personal data easily accessed without the need to trawl through a file.

2.2 'Personal Data' includes any information which relates to a living individual who can or may be identified from that information. Examples may include:

- An employee's name and address
- Date of birth
  - Statement of fact
  - Any expression or opinion communicated about an individual
  - Minutes of meetings, reports
  - Emails, file notes, handwritten notes, sticky notes
  - Spreadsheets and/or databases
  - Employment and education history

2.3 **'**Sensitive Personal Data**'** includes any information relating to an individual's:

- Ethnicity
- Gender
- Religious or other beliefs
- Political opinions
- Membership of a trade union
- Sexual orientation
- Medical history
- Offences committed or alleged to have been committed by that individual

2.4 'Data Subject' includes any living individual who is the subject of personal data whether in a personal or business capacity.

Palace for Life Foundation recognises and understands the consequences of failure to comply with the requirements of the Act may result in:

- Criminal and civil action;
- Fines and damages;
- Personal accountability and liability;

- Suspension/withdrawal of the right to process personal at by the Information Commissioners Office (ICO);
- Loss of confidence in the integrity of the Foundation's systems and procedures;
- Irreparable damage to CPFC/Palace for Life Foundation's reputation;
- Where staff do not comply with this policy, Palace for Life Foundation may also consider taking action in accordance with our established Disciplinary Procedure.

3. Staff Obligations

Staff will not gain access to information that is not necessary to hold, know or process. All information which is held will be relevant and accurate for the purpose for which it is required. The information will not be kept for longer than is necessary and will be kept secure at all times.

Staff will ensure that all personal or sensitive personal information is anonymised as part of any evaluation of assets and liability assessments except as required by law.

Staff who manage and process personal or sensitive information will ensure that it is kept secure and, where necessary, confidential. Sensitive personal information will only be processed in line with the provisions set out in this policy.

Staff are responsible for notifying their line manager or Palace for Life Foundation Business Support Manager if they believe or suspect that a conflict with this policy has occurred, or may occur in the future. This includes notification of any actual or suspected data breach.

4. Palace for Life Foundation (Data Controller) Obligations

i) Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, Palace for Life Foundation shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.

ii) Where proportionate in relation to processing activities, the measures referred to in paragraph (i) shall include the implementation of appropriate data protection policies by the controller.

iii) Adherence to approved codes of conduct as referred to in Article 40 of GDPR or approved certification mechanisms as referred to in Article 42 of GDPR may be used as an element by which to demonstrate compliance with the obligations of the controller.

5. Data Subjects' Rights

Palace for Life Foundation acknowledges individuals' (data subjects') rights under the Act to access any personal data held on our systems and in our files, upon their request. This includes deleting and/or correcting this information if it is proven to be inaccurate, excessive or out of date.

Palace for Life Foundation recognises that individuals have the right to make a request in writing and obtain a copy of their personal information if held on our systems and files. This request must be made without undue delay and within one month (extendable by two where complex/numerous).

Palace for Life Foundation recognises that individuals have the right:

- To restrict processing
- To object
- On automated decision making/profiling
- To data portability

- To erasure where personal data is no longer necessary, consent is withdrawn or data subject objects

Palace for Life Foundation will only share information in accordance with the provisions set out in the Act and where applicable the Foundation will inform individuals of the identity of third parties to whom we may share, disclose or be required to pass on information to, whilst accounting for any exemptions which may apply under the Act.

Complaints

Individuals who wish to make a complaint relating to breaches of the Data Protection Act 1998 and/or complaints that an individual's personal information is not being processed in line with this policy may do so in writing to:

Business Support Manager

Palace for Life Foundation

Selhurst Park

London

SE25 6PU

WEBSITE PRIVACY POLICY

CONTENTS

CLAUSE

Introduction

Welcome to the Palace for Life Foundation's privacy notice.

Palace for Life Foundation respects your privacy and is committed to protecting your personal data. This privacy notice will inform you as to how we look after your personal data when you visit our website (regardless of where you visit it from) and tell you about your privacy rights and how the law protects you.

This privacy notice is provided in a layered format so you can click through to the specific areas set out below. Please also use the Glossary to understand the meaning of some of the terms used in this privacy notice.

1. Important information and who we are

Purpose of this privacy notice

This privacy notice aims to give you information on how Palace for Life Foundation collects and processes your personal data through your use of this website, including any data you may provide through this website when you sign up to our newsletter, purchase a product or service or take part in a competition.

It is important that you read this privacy notice together with any other privacy notice or fair processing notice we may provide on specific occasions when we are collecting or processing personal data about you so that you are fully aware of how and why we are using your data. This privacy notice supplements the other notices and is not intended to override them.

Controller

Palace for Life Foundation is the controller and responsible for your personal data (collectively referred to as Palace for Life, "we", "us" or "our" in this privacy notice).

This privacy notice is issued on behalf of the Palace for Life Foundation so when we mention Palace for Life, "we", "us" or "our" in this privacy notice, we are referring to the relevant company in the Palace for Life Foundation responsible for processing your data. Palace for Life Foundation is the controller and responsible for this website.

We have appointed a data privacy manager who is responsible for overseeing questions in relation to this privacy notice. If you have any questions about this privacy notice, including

any requests to exercise your legal rights, please contact the data privacy manager using the details set out below.

Contact details

Our full details are:

Full name of legal entity: Palace for Life Foundation

Name/title of data privacy manager: Duncan Robinson/Business Support Manager

Email address: details@palaceforlife.org

Postal address: Selhurst Park, London, SE25 6PU

Telephone number: 020 8768 6047

You have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues (*www.ico.org.uk*). We would, however, appreciate the chance to deal with your concerns before you approach the ICO so please contact us in the first instance.

Changes to the privacy notice and your duty to inform us of changes

This version was last updated on 11th April 2018.

The data protection law in the UK will change on 25 May 2018. Although this privacy notice sets out most of your rights under the new laws, we may not yet be able to respond to some of your requests (for example, a request for the transfer of your personal data) until May 2018 as we are still working towards getting our systems ready for some of these changes.

It is important that the personal data we hold about you is accurate and current. Please keep us informed if your personal data changes during your relationship with us.

Third-party links

This website may include links to third-party websites, plug-ins and applications. Clicking on those links or enabling those connections may allow third parties to collect or share data about you. We do not control these third-party websites and are not responsible for their privacy

statements. When you leave our website, we encourage you to read the privacy notice of every website you visit.

2. The data we collect about you

Personal data, or personal information, means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data).

We may collect, use, store and transfer different kinds of personal data about you which we have grouped together follows:

- **Identity Data** includes first name, maiden name, last name, username or similar identifier, marital status, title, date of birth and gender.

- **Contact Data** includes billing address, delivery address, email address and telephone numbers.

- **Financial Data** includes bank account and payment card details.

- **Transaction Data** includes details about payments to and from you and other details of products and services you have purchased from us.

- **Technical Data** includes internet protocol (IP) address, your login data, browser type and version, time zone setting and location, browser plug-in types and versions, operating system and platform and other technology on the devices you use to access this website.

- **Profile Data** includes your username and password, purchases or orders made by you, your interests, preferences, feedback and survey responses.

- **Usage Data** includes information about how you use our website, products and services.

- **Marketing and Communications Data** includes your preferences in receiving marketing from us and our third parties and your communication preferences.

We also collect, use and share **Aggregated Data** such as statistical or demographic data for any purpose. Aggregated Data may be derived from your personal data but is not considered personal data in law as this data does **not** directly or indirectly reveal your identity. For example, we may aggregate your Usage Data to calculate the percentage of users accessing a specific website feature. However, if we combine or connect Aggregated Data with your personal data so that it can directly or indirectly identify you, we treat the combined data as personal data which will be used in accordance with this privacy notice.

We may, where relevant, collect **Special Categories of Personal Data** about you, this includes details about your race or ethnicity, religious or philosophical beliefs, sexual orientation, information about your health and genetic and biometric data.

If you fail to provide personal data

Where we need to collect personal data by law, or under the terms of a contract we have with you and you fail to provide that data when requested, we may not be able to perform the contract we have or are trying to enter into with you (for example, to provide you with goods or services). In this case, we may have to cancel a product or service you have with us but we will notify you if this is the case at the time.

3. How is your personal data collected?

We use different methods to collect data from and about you including through:

- **Direct interactions.** You may give us your Identity, Contact and Financial Data by filling in forms or by corresponding with us by post, phone, email or otherwise. This includes personal data you provide when you:
- apply for our products or services;
- create an account on our website;
- subscribe to our service or publications;
- request marketing to be sent to you;
- enter a competition, promotion or survey; or
- give us some feedback.
- **Automated technologies or interactions.** As you interact with our website, we may automatically collect Technical Data about your equipment, browsing actions and patterns. We collect this personal data by using cookies, server logs and other similar technologies. We may also receive Technical Data about you if you visit other websites employing our cookies.
- **Third parties or publicly available sources.** We may receive personal data about you from various third parties and public sources as set out below:
- Technical Data from the following parties:

(a) analytics providers;

(b) advertising networks; and

(c) search information providers.

- Contact, Financial and Transaction Data from providers of technical, payment and delivery services.
- Identity and Contact Data from data brokers or aggregators (including referrals).
- Identity and Contact Data from publicly availably sources.

4. How we use your personal data

We will only use your personal data when the law allows us to. Most commonly, we will use your personal data in the following circumstances:

- Where we need to perform the contract we are about to enter into or have entered into with you.
- Where it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests.
- Where we need to comply with a legal or regulatory obligation.

Click here to find out more about the types of lawful basis that we will rely on to process your personal data.

Generally we do not rely on consent as a legal basis for processing your personal data other than in relation to sending third party direct marketing communications to you via email or text message. You have the right to withdraw consent to marketing at any time by contacting us.

Purposes for which we will use your personal data

We have set out below, in a table format, a description of all the ways we plan to use your personal data, and which of the legal bases we rely on to do so. We have also identified what our legitimate interests are where appropriate.

Note that we may process your personal data for more than one lawful ground depending on the specific purpose for which we are using your data. Please contact us if you need details about the specific legal ground we are relying on to process your personal data where more than one ground has been set out in the table below.

Purpose/Activity	**Type of data**	**Lawful basis for processing including basis of legitimate interest**
To register you as a new customer	(a) Identity (b) Contact	Performance of a contract with you
To process and deliver your order including: (a) Manage payments, fees and charges (b) Collect and recover money owed to us	(a) Identity (b) Contact (c) Financial (d) Transaction (e) Marketing and Communications	(a) Performance of a contract with you (b) Necessary for our legitimate interests (to recover debts due to us)
To manage our relationship with you which will include:	(a) Identity (b) Contact (c) Profile	(a) Performance of a contract with you

(a) Notifying you about changes to our terms or privacy policy (b) Asking you to leave a review or take a survey	(d) Marketing and Communications	(b) Necessary to comply with a legal obligation (c) Necessary for our legitimate interests (to keep our records updated and to study how customers use our products/services)
To enable you to partake in a prize draw, competition or complete a survey	(a) Identity (b) Contact (c) Profile (d) Usage (e) Marketing and Communications	(a) Performance of a contract with you (b) Necessary for our legitimate interests (to study how customers use our products/services, to develop them and grow our business)
To administer and protect our business and this website (including troubleshooting, data analysis, testing, system maintenance, support, reporting and hosting of data)	(a) Identity (b) Contact (c) Technical	(a) Necessary for our legitimate interests (for running our business, provision of administration and IT services, network security, to prevent fraud and in the context of a business reorganisation or group restructuring exercise) (b) Necessary to comply with a legal obligation
To deliver relevant website content and advertisements to you and measure or understand the effectiveness of the advertising we serve to you	(a) Identity (b) Contact (c) Profile (d) Usage (e) Marketing and Communications (f) Technical	Necessary for our legitimate interests (to study how customers use our products/services, to develop them, to grow our business and to inform our marketing strategy)
To use data analytics to improve our website, products/services, marketing, customer relationships and experiences	(a) Technical (b) Usage	Necessary for our legitimate interests (to define types of customers for our products and services, to keep our website updated and relevant, to develop our business and to inform our marketing strategy)
To make suggestions and recommendations to you	(a) Identity (b) Contact	Necessary for our legitimate interests (to develop our

about goods or services that may be of interest to you	(c) Technical (d) Usage (e) Profile	products/services and grow our business)

Marketing

We strive to provide you with choices regarding certain personal data uses, particularly around marketing and advertising. We have established the following personal data control mechanisms:

Promotional offers from us

We may use your Identity, Contact, Technical, Usage and Profile Data to form a view on what we think you may want or need, or what may be of interest to you. This is how we decide which products, services and offers may be relevant for you (we call this marketing).

You will receive marketing communications from us if you have requested information from us or purchased goods or services from us or if you provided us with your details when you entered a competition or registered for a promotion and, in each case, you have not opted out of receiving that marketing.

Third-party marketing

We will get your express opt-in consent before we share your personal data with any company outside the Palace for Life group of companies for marketing purposes.

Opting out

You can ask us or third parties to stop sending you marketing messages at any time by contacting us at any time.

Where you opt out of receiving these marketing messages, this will not apply to personal data provided to us as a result of a product/service purchase, warranty registration, product/service experience or other transactions.

Cookies

You can set your browser to refuse all or some browser cookies, or to alert you when websites set or access cookies. If you disable or refuse cookies, please note that some parts of this website may become inaccessible or not function properly.

Change of purpose

We will only use your personal data for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible

with the original purpose. If you wish to get an explanation as to how the processing for the new purpose is compatible with the original purpose, please contact us.

If we need to use your personal data for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

Please note that we may process your personal data without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

5. Disclosures of your personal data

We may have to share your personal data with the parties set out below for the purposes set out in the table in paragraph 4 above.

- Internal Third Parties as set out in the Glossary.
- External Third Parties as set out in the Glossary.
- Specific third parties acting as processors.
- Third parties to whom we may choose to sell, transfer, or merge parts of our business or our assets. Alternatively, we may seek to acquire other businesses or merge with them. If a change happens to our business, then the new owners may use your personal data in the same way as set out in this privacy notice.

We require all third parties to respect the security of your personal data and to treat it in accordance with the law. We do not allow our third-party service providers to use your personal data for their own purposes and only permit them to process your personal data for specified purposes and in accordance with our instructions.

6. International transfers

Whenever we transfer your personal data out of the EEA, we ensure a similar degree of protection is afforded to it by ensuring at least one of the following safeguards is implemented:

- Where we use providers based in the US, we may transfer data to them if they are part of the Privacy Shield which requires them to provide similar protection to personal data shared between the Europe and the US. For further details, see *European Commission: EU-US Privacy Shield*.

Please contact us if you want further information on the specific mechanism used by us when transferring your personal data out of the EEA.

7. Data security

We have put in place appropriate security measures to prevent your personal data from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal data to those employees, agents, contractors and other third

parties who have a business need to know. They will only process your personal data on our instructions and they are subject to a duty of confidentiality.

We have put in place procedures to deal with any suspected personal data breach and will notify you and any applicable regulator of a breach where we are legally required to do so.

8. Data retention

How long will you use my personal data for?

By law we have to keep basic information about our customers (including Contact, Identity, Financial and Transaction Data) for seven years after they cease being customers for tax purposes.

In some circumstances you can ask us to delete your data: see *Request erasure* below for further information.

In some circumstances we may anonymise your personal data (so that it can no longer be associated with you) for research or statistical purposes in which case we may use this information indefinitely without further notice to you.

9. Your legal rights

Under certain circumstances, you have rights under data protection laws in relation to your personal data. Please click on the link below to find out more about these rights:

Individual Rights

If you wish to exercise any of the rights set out above, please contact us.

No fee usually required

You will not have to pay a fee to access your personal data (or to exercise any of the other rights). However, we may charge a reasonable fee if your request is clearly unfounded, repetitive or excessive. Alternatively, we may refuse to comply with your request in these circumstances.

What we may need from you

We may need to request specific information from you to help us confirm your identity and ensure your right to access your personal data (or to exercise any of your other rights). This is a security measure to ensure that personal data is not disclosed to any

person who has no right to receive it. We may also contact you to ask you for further information in relation to your request to speed up our response.

Time limit to respond

We try to respond to all legitimate requests within one month. Occasionally it may take us longer than a month if your request is particularly complex or you have made a number of requests. In this case, we will notify you and keep you updated.

10. Glossary

LAWFUL BASIS

Legitimate Interest means the interest of our business in conducting and managing our business to enable us to give you the best service/product and the best and most secure experience. We make sure we consider and balance any potential impact on you (both positive and negative) and your rights before we process your personal data for our legitimate interests. We do not use your personal data for activities where our interests are overridden by the impact on you (unless we have your consent or are otherwise required or permitted to by law). You can obtain further information about how we assess our legitimate interests against any potential impact on you in respect of specific activities by contacting us.

Performance of Contract means processing your data where it is necessary for the performance of a contract to which you are a party or to take steps at your request before entering into such a contract.

Comply with a legal or regulatory obligation means processing your personal data where it is necessary for compliance with a legal or regulatory obligation that we are subject to.

THIRD PARTIES

Internal Third Parties

Other companies in the Palace for Life Group acting as joint controllers or processors and provide IT and system administration services and undertake leadership reporting.

External Third Parties

- Service providers acting as processors who provide IT and system administration services.
- Professional advisers acting as processors or joint controllers including lawyers, bankers, auditors and insurers who provide consultancy, banking, legal, insurance and accounting services.
- HM Revenue & Customs, regulators and other authorities acting as processors or joint controllers based in the United Kingdom who require reporting of processing activities in certain circumstances.

YOUR LEGAL RIGHTS

You have the right to:

Request access to your personal data (commonly known as a "data subject access request"). This enables you to receive a copy of the personal data we hold about you and to check that we are lawfully processing it.

Request correction of the personal data that we hold about you. This enables you to have any incomplete or inaccurate data we hold about you corrected, though we may need to verify the accuracy of the new data you provide to us.

Request erasure of your personal data. This enables you to ask us to delete or remove personal data where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal data where you have successfully exercised your right to object to processing (see below), where we may have processed your information unlawfully or where we are required to erase your personal data to comply with local law. Note, however, that we may not always be able to comply with your request of erasure for specific legal reasons which will be notified to you, if applicable, at the time of your request.

Object to processing of your personal data where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground as you feel it impacts on your fundamental rights and freedoms. You also have the right to object where we are processing your personal data for direct marketing purposes. In some cases, we may demonstrate that we have compelling legitimate grounds to process your information which override your rights and freedoms.

Request restriction of processing of your personal data. This enables you to ask us to suspend the processing of your personal data in the following scenarios: (a) if you want us to establish the data's accuracy; (b) where our use of the data is unlawful but you do not want us to erase it; (c) where you need us to hold the data even if we no longer require it as you need it to establish, exercise or defend legal claims; or (d) you have objected to our use of your data but we need to verify whether we have overriding legitimate grounds to use it.

Request the transfer of your personal data to you or to a third party. We will provide to you, or a third party you have chosen, your personal data in a structured, commonly used, machine-readable format. Note that this right only applies to automated information which you initially provided consent for us to use or where we used the information to perform a contract with you.

Withdraw consent at any time where we are relying on consent to process your personal data. However, this will not affect the lawfulness of any processing carried out before you withdraw your consent. If you withdraw your consent, we may not be able to provide certain products or services to you. We will advise you if this is the case at the time you withdraw your consent.

SECURITY POLICY FOR PAYMENT CARD INDUSTRY (PCI)

Policy Statement

All card processing activities and related technologies must comply with the Payment Card Industry Data Security Standard (PCI-DSS) in its entirety. Card processing activities must be conducted as described herein and in accordance with the standards and procedures listed in the Related Documents section of this Policy. No activity may be conducted nor any technology employed that might obstruct compliance with any portion of the PCI-DSS.

This policy shall be reviewed at least annually and updated as needed to reflect changes to business objectives or the risk environment.

1 Applicability and Availability

This policy applies to all employees. Relevant sections of this policy apply to vendors, contractors, and business partners. The most current version of this policy is available on the CPFC Intranet or in the Employee Handbook.

2 Adherence to Standards

Configuration standards must be maintained for applications, network components, critical servers, and wireless access points. These standards must be consistent with industry-accepted hardening standards as defined, for example, by SysAdmin Assessment Network Security Network (SANS), National Institute of Standards Technology (NIST), and Center for Internet Security (CIS).

Configuration standards must include:

- updating of anti-virus software and definitions
- provision for installation of all relevant new security patches within 30 days
- prohibition of group and shared passwords

3 Handling of Cardholder Data

Distribution, maintenance, and storage of media containing cardholder data, must be controlled, including that distributed to individuals. Procedures must include periodic media inventories in order to validate the effectiveness of these controls.

Procedures for data retention and disposal must be maintained by each department and must include the following:

- legal, regulatory, and business requirements for data retention, including specific requirements for retention of cardholder data
- provisions for disposal of data when no longer needed for legal, regulatory, or business reasons, including disposal of cardholder data
- coverage for all storage of cardholder data, including database servers, mainframes, transfer directories, and bulk data copy directories used to transfer data between servers, and directories used to
- a programmatic (automatic) process to remove, at least on a quarterly basis, stored cardholder data that exceeds business retention requirements, or, alternatively, an audit process, conducted at least on a quarterly basis, to verify that stored cardholder data does not exceed business retention requirements
- destruction of media when it is no longer needed for business or legal reasons as follows:
    - cross-cut shred, incinerate, or pulp hardcopy materials
    - purge, degauss, shred, or otherwise destroy electronic media such that data cannot be reconstructed

Credit card numbers must be masked when displaying cardholder data. Those with a need to see full credit card numbers must request an exception to this policy using the exception process.

Unencrypted Primary Account Numbers may not be sent via email

4 Access to Cardholder Data

Procedures for data control must be maintained by each department and must incorporate the following:

- Access rights to privileged User IDs are restricted to least privileges necessary to perform job responsibilities
- Assignment of privileges is based on individual personnel's job classification and function
- Requirement for an authorization form signed by management that specifies required privileges
- Implementation of an automated access control system

5 Critical Employee-facing Technologies

For critical employee-facing technologies, departmental procedures shall require:

- explicit management approval to use the devices
- that all device use is authenticated with username and password or other authentication item (for example, token)
- a list of all devices and personnel authorized to use the devices

- labeling of devices with owner, contact information, and purpose
- automatic disconnect of modem sessions after a specific period of inactivity
- activation of modems used by vendors only when needed by vendors, with immediate deactivation after use

Departmental usage standards shall include:
- acceptable uses for the technology
- acceptable network locations for the technology
- a list of company-approved products
- prohibition of the storage of cardholder data onto local hard drives, floppy disks, or other external media when accessing such data remotely via modem
- prohibition of use of cut-and-paste and print functions during remote access

6 Responsibilities

Will maintain daily operational security procedures consistent with this the PCI-DSS, including administrative and technical procedures for each of the requirements

Management Accountant is responsible for overseeing all aspects of information security, including but not limited to:
- creating and distributing security policies and procedures
- monitoring and analysing security alerts and distributing information to appropriate information security and business unit management personnel
- creating and distributing security incident response and escalation procedures that include:
    - roles, responsibilities, and communication
    - coverage and responses for all critical system components
    - notification, at a minimum, of credit card associations and acquirers
    - strategy for business continuity post compromise
    - reference or inclusion of incident response procedures from card associations
    - analysis of legal requirements for reporting compromises
    - annual testing
    - designation of personnel to monitor for intrusion
    - detection, intrusion prevention, and file integrity monitoring alerts on a 24/7 basis
    - plans for periodic training
    - a process for evolving the incident response plan according to lessons learned and in response to industry developments
- maintaining a formal security awareness program for all employees that provides
- multiple methods of communicating awareness and educating employees (for example, posters, letters, meetings)
- review security logs at least daily and follow-up on exceptions

The Management Accountant shall maintain daily administrative and technical operational security procedures that are consistent with the PCI-DSS (for example, user account maintenance procedures, and log review procedures).

System and Application Administrators shall:

- Monitor and analyse security alerts and information and distribute to appropriate personnel
- administer user accounts and manage authentication
- monitor and control all access to data
- maintain a list of connected entities
- perform due diligence prior to connecting an entity, with supporting documentation
- verify that the entity is PCI-DSS compliant, with supporting documentation
- establish a documented procedure for connecting and disconnecting entities
- retain audit logs for at least one year

The Management Accountant is responsible for tracking employee participation in the security awareness program, including:

- facilitating participation upon hire and at least annually
- ensuring that employees acknowledge in writing that they have read and understand the company's information security policy
- screen potential employees to minimise the risk of attacks from internal sources

Internal Audit is responsible for executing a risk assessment process that identifies threats, vulnerabilities, and results in a formal risk assessment.

The Head of Foundation will ensure that for service providers with whom cardholder information is shared:

- contracts require adherence to PCI-DSS by the service provider
- contracts include acknowledgement or responsibility for the security of cardholder data by the service provider

7 Related Documents

Data Protection Policy
IT & Software Policy
Disciplinary and Grievance Procedures
Confidentiality and Non-Disclosure Policy
Anti-bribery policy