Lee Valley Regional Park Authority	Agenda Item No:
LEE VALLEY REGIONAL PARK AUTHORITY	8
AUTHORITY MEETING	Report No:
22 OCTOBER 2020 AT 14:00	**A/4285/20**

INFORMATION TECHNOLOGY POLICIES UPDATE

Presented by the Head of IT

EXECUTIVE SUMMARY

The purpose of this report is to seek Member approval for the revised IT Usage Policy and Information and Security Policy that have been updated as part of a review of all the Authority's existing policies. The policies have been updated to take account of legislative changes, best practice and the Authority's business objectives. Executive Committee have approved the revised policies for recommendation to Authority (Paper E/685/20).

RECOMMENDATIONS

Members Approve:

(1) the IT Usage Policy attached at Appendix A of this report; and

(2) the Information and Security Policy attached at Appendix B of this report.

BACKGROUND

1 The Authority has a register of policies that ensure the organisation works efficiently and consistently towards delivering its Business Strategy. These policies are reviewed to ensure they are relevant and up to date with legislation and best practice.

2 It should be noted that the Authority implements legislative changes from the date they are introduced; and there may be a time lag between this and the relevant policies being updated.

IT USAGE POLICY

3 A draft of the revised IT Usage Policy is attached at Appendix A to this report for Members' consideration and approval.

4 The IT Usage Policy defines the acceptable use of IT equipment and related services, systems and facilities by providing clear guidance as to what is, and what is not, acceptable behaviour in the use of IT systems.

5 The most significant change to the IT Usage Policy is the removal of the procedural elements, for which separate procedures have now been created.

6 The procedural elements that have been removed and are now separate procedures are as follows:

- Authority Email Procedure;
- I.T User Access Procedure;
- Mobile Phone Procedure;
- Database Design Procedure;
- Intranet guidelines;
- Internet Usage Procedure; and
- IT Hardware procedure.

7 Other changes include the Change of Author and Sponsor of the Policy, updating of terminology, consolidation of content and references to post names, where they have been changed following the recent restructure (for example I.T Manager has been changed to Head of IT).

8 The aim of the proposed policy is to ensure that staff use IT systems and equipment in the proper and appropriate manner and to reduce the risk of Cyber-attacks.

INFORMATION AND SECURITY POLICY

9 A draft of the revised Information and Security Policy is attached at Appendix B of this report for Members' consideration and approval.

10 The Information and Security Policy sets out the Authority's high level requirements for the management of Information Security across the organisation in relation to the storage, processing and transmission of payment card data.

11 The policy has been updated to reflect the changes in ownership of Payment Card Industry (PCI) compliance following the end of the Leisure Services Contract with Lee Valley Leisure Trust Ltd.

12 One significant change is the removal of the use of carbon paper slips to support card transactions when used for emergencies (I.e. when there is no network connection for Chip & Pin), as they are no longer acceptable under the PCI standards of compliance. This was previously referenced under the storing of card data section of the Policy.

13 Other changes include:

- change of Author and Sponsor of the Policy;
- update to the reporting structure (section 5.1) and associated teams (section 5.2) to the appropriate Authority officers;
- updated who can approve what card payment systems (Card payment systems section 4.2);
- the requirement of third party vendors to provide a valid Attestation of Compliance (AOC) as proof of their PCI/DSS compliance (Data Confidentiality for Service Providers / Third Parties section); and
- added the statement that card details must never be sent unencrypted (Transmitting card data section).

14 The aim of the proposed policy is to ensure that the Authority complies with the relevant legislation.

ENVIRONMENTAL IMPLICATIONS

15 There are no environmental implications arising directly from the recommendations in this report.

FINANCIAL IMPLICATIONS

16 There are no financial implications arising directly from the recommendations in this report.

HUMAN RESOURCE IMPLICATIONS

17 The new policies will be communicated to all staff and the Authority will ensure that managers are adequately trained to implement the procedures in accordance with these policies.

LEGAL IMPLICATIONS

18 The legal implications are set out in the body of this report.

RISK MANAGEMENT IMPLICATIONS

19 There are no risk management implications arising directly from the recommendations in this report.

Author: Simon Clark, 01992 709 893, sclark@leevalleypark.org.uk

APPENDICES ATTACHED

Appendix A	IT Usage Policy
Appendix B	Information and Security Policy

LIST OF ABBREVIATIONS

IT	Information Technology
PCI	Payment Card Industry
Carbon paper slips	Carbon paper slips are used with credit card imprinter machines for the bank, merchant and customer as proof of purchase
AOC	Attestation of Compliance

PREVIOIUS COMMITTEE REPORT

Executive	E/685/20	Information Technology Policies Update	24 September 2020

This page is blank

IT Usage Policy
Information Technologies (IT)
Lee Valley Regional Park Authority

Lee Valley Regional Park Authority

IT Usage Policy

Issue 7

Detail

This procedure covers the following points:

Lee Valley Regional Park Authority

IT Usage Policy

Issue 7

Version Control

Updated on	Details	Updated by	Issue No
September 2008	Approved by Members 25/09/08 (Paper FA/175/08)		1.0
October 2013	Circulated to Policy and Procedure Review Group for discussions		1.0
November 2013	Comments from P&P Review Group		1.0
December 2013	Version for Exchange to review.		1.0
May 2015	Updated Backup Section	Simon Clark	1.1
09/07/15	Updated Mobile device section	Simon Clark	2
18/09/15	Updates following Policy working group meeting	Simon Clark	3
26/10/15	Updated with details and changes made by Simon Sheldon	Simon Clark	4
12/12/17	Major update to document, Including information and layout	Simon Clark	5
17/10/19	Review and update	Simon Clark	6
04/09/20	Review and update	Simon Clark	7

Document Information

Consultation: Policy & Procedure Review Group

Approved by: Authority Members
Approval Date:

Review Frequency: Every 3 Years
Next Review: October 2023

Author	Simon Clark – Head of Information Technology □□ sclark@leevalleypark.org.uk □□ □ (01992) 709893 or x893
Sponsor	Daniel Buck – Corporate Director □□ dbuck@leevalleypark.org.uk □□ □ (01992) 709896 or x896
Consultation:	Legal & Information Officer HR Manager Policy & Procedure Review Group
Approved	**Approved by:** Authority **Approval Date:** XXXXXXXXX **Review Frequency:** Every Year **Next Review:** September 2014

Commented [CS1]: Was previously IT Manager Point 7

Commented [CS2]: Was previously Corporate Director of Finance Point 7

Lee Valley Regional Park Authority

IT Usage Policy

Issue 7

Overview

The purpose of this policy is to describe the acceptable use of IT equipment and related services, systems and facilities by providing clear guidance as to what is, and what is not, acceptable behaviour in the use of IT systems.

The Policy is maintained and regulated by Lee Valley Regional Park Authority (LVRPA) and is cross-referenced to, and by, a number of other LVRPA policies and regulations, in particular, the Data Protection Act 1998, the Regulation of Investigatory Powers Act 2000, the Freedom of Information Act 2000 and the Human Rights Act 1998.

Users are reminded that this policy has been written in the context of the basic laws of the land, which have been strengthened over the past few years to cover these areas.

The Chief Executive of LVRPA is responsible for ensuring that this policy and related procedures are up-to-date, relevant and are adhered to by all users of IT equipment within LVRPA.

The Policy will be made available to users of any IT system (email and related services and facilities) and will be reviewed every three years, or before if there is a need i.e. legislation. This will be necessary with regard to the expected development of the system, the operational use of the system and generally recognised best practice.

Introduction

This policy applies to everyone who has access to Information Technology (IT) systems used by LVRPA whether in the work place or at home, whether employee, contractor, volunteer or any other designated user.

All IT assets are owned, managed and operated by LVRPA and are for use in relation to work carried out for the Authority. Users of IT systems and equipment, must understand and accept responsibility for the security and protection of IT assets (whether use of IT systems, mobile phones, IT equipment, confidentiality of data, or the processing of paper documents), by signing this IT Usage Policy.

The following procedures must be read in conjunction with the IT Usage Policy before signing the declaration:

- Authority Email Procedure
- I.T User Access Procedure
- Mobile Phone Procedure
- Database Design Procedure
- Intranet guidelines
- Internet Usage Procedure
- IT Hardware procedure

Commented [CS3]: These procedures were previously included within the Policy. They have now been removed and had individual procedures created.
Point 6

Lee Valley Regional Park Authority

IT Usage Policy

Issue 7

Definitions

For the purpose of this document, the term 'IT', 'IT Equipment' or 'IT Systems' will cover; desktop computers, laptops, notebooks, tablets, telephones (including mobile phones and iPhones), printers, routers, servers, e-mail accounts and any other associated hardware and software in use both directly or indirectly.

For the purpose of this document, the term 'users' and 'staff' will mean; employees, agency staff, voluntary workers, LVRPA Members and contractors.

Statement of Trust

This policy is intended to detail the rules of conduct for all users of LVRPA who use IT. equipment. This policy applies to the use of any IT system, including hardware, software and networks, provided by LVRPA. The Policy is applicable to all users.

Only authorised users of LVRPA are entitled to use its IT equipment. All users of LVRPA, who agree and abide by LVRPA regulations, are able to use computing facilities and email systems at all times when the network is available.
LVRPA complies with and adheres to all its current legal responsibilities including Data Protection, Electronic Communication, Regulation of Investigatory Powers (RIP), Human Rights, Computer Misuse, Copyright and Intellectual Property.

Statement of Responsibilities

All Managers will be responsible for ensuring their staff are aware of this policy.
Individual users are responsible for their own actions. The use of IT equipment by individuals within LVRPA assumes and implies compliance with this policy, without exception, and those Acts, Policies and Regulations referenced above and enacted or authorised by LVRPA or other regulatory bodies. Every user has a duty to ensure they practice appropriate and proper use and must understand their responsibilities in this regard.
IT equipment and software should only be used in accordance with this policy and associated polices and not in any way that will bring LVRPA into disrepute.

IT equipment should be looked after as if it were the users own property and kept secure when not in use. Only designated users of LVRPA are authorised to use LVRPA equipment. This means it must not be used by either family or friends.

Any loss or damage to LVRPA' IT equipment must be reported to the IT section immediately. Any loss or damage of equipment which is attributable to the negligence or irresponsible use by the user will require that individual to reimburse LVRPA for the full replacement cost of that equipment.

The IT equipment available is provided for the efficient performance of LVRPA' business. Irresponsible use of IT or failure to take reasonable care will become a disciplinary matter.

Lee Valley Regional Park Authority

IT Usage Policy

Issue 7

General Computer Usage

IT equipment is issued to allow users to undertake their work duties and should be considered as work equipment. Any equipment can be removed by IT without notice or recompense.

Acceptable Use of IT Equipment

Users must look after and/or maintain any IT equipment that is issued to them. It will be deemed to be inappropriate to use the equipment in a way that is not befitting of the item.

Users must not access, download, upload, post (on websites) or transmit any material which might reasonably be considered to be obscene, abusive, sexist, racist, defamatory, libellous, intentionally false or inaccurate or inappropriate. If a user receives such material, they should report the matter to the IT Manager immediately, who will then contact the relevant line manager to make them aware of the situation. Disciplinary action will be taken against anyone who is found to be sending such material.

PC's and associated equipment must be kept clean and in good general physical condition. Cleaning materials can be purchased from LVRPA' stationery suppliers, the cost of which will be paid for out of individual department budgets. Personalisation of IT equipment is not permitted, this includes use of stickers and markings.

Food and drink should not be placed on any IT equipment and users should take care when consuming food and drink when in close proximity to IT equipment. Food and Drink must not be consumed in any of the venues server rooms.

When transporting IT equipment, for example, a laptop in a user's car, it must be stored in the boot of the vehicle and be out of visible sight. The boot of the car must, where possible, be kept locked at all times even when you are driving. On arrival at the destination the IT equipment should be removed from the vehicle as far as is practically possible.

The ability to connect to other computer systems through the network does not imply a right to connect to those systems or to make use of those systems unless authorised to do so. Users must not alter or copy a file that is write protected (belonging to another user) without first obtaining written permission from the creator of the file.

Any perceived intended or intentional damage caused to any IT equipment will be viewed as unacceptable and will result in access to that equipment being removed completely and any damage paid for.

Lee Valley Regional Park Authority

IT Usage Policy

Issue 7

User Information

It is the responsibility of the user to ensure that information such as name, job title, phone number etc. is correct. Changes to job titles must be approved by HR before being applied by IT.

Compliance

Failure to comply with any of the provisions of this usage policy will result in disciplinary action in accordance with the normal procedures of LVRPA.

Incident Handling and Data Protection

LVRPA will investigate complaints received from both internal and external sources, about any unacceptable use of IT equipment or resources. User accounts may be closed or disabled and email may be blocked or disabled to prevent further damage or similar incidents occurring.

Queries

If you have any queries about this policy or IT usage generally, please contact the IT Manager.

Please now sign the IT Usage Policy declaration and return (only the signed declaration) to the IT Department.

Lee Valley Regional Park Authority

IT Usage Policy Declaration

The IT. Usage Policy may alter from time to time and the updated IT. Usage Policy will be available on Compass. Please review the IT. Usage Policy regularly to ensure you are aware of any changes. Your continued use of IT. equipment, services and systems after changes are posted means you agree to this IT. Usage Policy as updated and/or amended.

I confirm that I have read, understood, accept and will abide by the requirements as set out in the IT. Usage Policy and associated procedures.

I confirm that any personally owned equipment that I may use to carry out LVRPA work has up to date Antivirus/Malware software installed, which I will ensure is regularly kept up to date.

User accounts will not be activated until this declaration has been received.

Declaration

Print Name (Capital letters).....

Department/Venue.....

Signature.....Date.....

Please return this signed declaration

Email scanned copy to:
helpdesk@leevalleypark.org.uk

or

Hard Copy to:
IT Department,
Lee Valley Regional Park Authority,
Myddelton House,
Bulls Cross,
Enfield, EN2 9HG

Lee Valley
Regional Park Authority

Information Security (Electronic Payments) Policy

September 2020

Reference: [Version 1]

This document is controlled by Lee Valley Regional Park Authority.

Lee Valley Regional Park Authority,
Myddelton House, Bulls Cross,
Enfield, Middlesex, EN2 9HG

THIS PAGE IS INTENTIONALLY BLANK

Appendix B to Paper A/4285/20

I Document Information

Title: **Information Security (Electronic Payments) Policy**

Status: Final Version

Current Version: v1 (September 2013)

Author	Simon Clark – Head of Information Technology sclark@leevalleypark.org.uk ☎ (01992) 709893 or x893
Sponsor	Daniel Buck – Corporate Director dbuck@leevalleypark.org.uk ☎ (01992) 709896 or x896
Consultation:	Legal & Information Officer HR Manager Policy & Procedure Review Group
Approved	**Approved by:** Authority **Approval Date:** XXXXXXXXX **Review Frequency:** Every Year **Next Review:** September 2014

Commented [CS1]: Change of Author (Point 13)
Was Nigel Foxall

Commented [CS2]: Change of Sponsor (Point 13)
Was Kulvinder Sihota

Version History		
Version	**Date**	**Description**
0.1	5 August 2013	First draft document prepared
0.2	2 September 2013	Circulated for comment
1	9 September 2013	Executive
1	October 2013	Authority
2	September 2020	Review and revision of Policy

II Contents

1. Introduction

1.1 This document details the security policy for the Authority in relation to the storage, processing and transmission of payment card data. Its aim is to provide a detailed understanding of Information Security responsibilities for all levels of staff, contractors, partners and third parties who access the Authority payment card processing network.

1.2 As part of the Authority's Payment Card Industry (PCI) Compliance programme, consideration has been made to payment card processing operations. Guidelines and controls form an essential part of the Authority's compliance status against the PCI Data Security Standard.

2. Policy Statement

2.1 This Lee Valley Regional Park Authority (Authority) Information Security Policy:

- Sets out the Authority's high level requirements for the management of Information Security across the organisation in relation to the storage, processing and transmission of payment card data.
- Defines the Information Security Policy for the organisation in line with Requirement 12 of the Payment Card Industry Data Security Standard (PCI DSS), to "maintain a policy that addresses information security for all personnel".
- Applies to all Payment Card Processing operations for the organisation.

2.2 This policy should be read in conjunction, with the Financial Regulations and Quality Management System (QMS) processes for:

- Cash and banking
- Cash Transactions

Note: wherever a statement in this policy refers to 'Card', the statement applies to credit, debit and charge cards, unless specifically stated otherwise.

3. Scope

3.1 This document should be reviewed by staff involved with the Authority's payment card processing operations. Specifically:

- Day-to-day payment card processing operations (including IT systems).
- Implementation of new payment card processing systems.
- Maintenance of existing payment card processing.

3.2 This document should also be used for reference purposes when the Authority undertakes its annual PCI compliance review.

4. Requirements

4.1 This policy deals with the controls required over the transmission, processing, and storage of all cardholder data and information received in respect of all card transactions accepted by the Authority. It applies to all entities that store, process and/or transmit cardholder data and covers technical and operational system components included in or connected to cardholder data

4.2 Key controls for controlling this cardholder data are as follows:

- **Card payment systems:** only E-PoS, E-Commerce and Pin Entry Devices (PED's) approved by the Head of Finance and compliant with PCI DSS systems can be used for Authority card payments.

Commented [CS3]: Updated who can approve what card payment systems from Corporate Director of Resources to Head of Finance: Point 13

- **Receiving or obtaining card data:** Card data must only be received by the methods of:
  - Customer Present (chip & pin) transactions, where the customer is able to enter their card details directly into the PED; or
  - Customer Not Present, via telephone where the card details are received and entered immediately into the card terminal; or
  - Via the online e-commerce system.

- **Transmitting card data:**
  - Card details must never be sent/received by email or by any other electronic method,
  - Card details must never be sent unencrypted,
  - Card details must never be entered into any online payment system other than that approved by the Authority.

Commented [CS4]: New addition to Policy: Point 13

- **Storing Card Data:**
  - Sensitive card data must never be retained on Authority computers after being used for processing,
  - No records of card security details or Authentication data, such as the 3-digit security card verification codes (CVC), and any other authentication data may be kept on Authority computers or in paper form,
  - No other records of customer's card details (e.g. database/spread sheet incorporating customer card information) are to be kept on Authority computers.
  - No track data (card electronic data) may be stored,
  - Card security details must never be stored in any computer application.

Commented [CS5]: Updated from: Till rolls and carbons (when used for emergencies) supporting card transactions can be stored, as long as they are held with access restricted to authorised personnal only.
Ref on report: Point 12

- **Card data received and processed online:**

  - Only the Authority approved online payment facility may be used for payment by credit card online.
  - The E-commerce system must be compliant with PCI DSS requirements and this policy.

- **Obtaining card details in other circumstances:** In certain cases, where prior approval has been received, card details may be taken as follows:

  - By post, on an order form, in which case the details should be immediately processed through an E-PoS and the card transaction processed, the card detail's part of the order form is then immediately destroyed by shredding.
  - By fax, in which case the faxed card details should be received directly by the Customer Services Assistant (CSA) and then immediately processed onto an E-PoS and the card transaction processed, the fax with the card details should then be destroyed.

- **Following card machine instructions:** As part of any card transaction the device may instruct an action by the operator which must be followed.

- **Staff with cardholder data access:**
  Access to any booking system and the associated payment card system and cardholder data will be limited to those staff whose job requires such access. Training will be provided to ensure these staff are aware of the significance of the data being held and the repercussions of disclosing it to those who do not need to know. Each such user will be issued with unique ID to access the booking system which must be used solely by the issued user.

- **Irregularities detected:**
  Any non-compliance with this policy document, or any other irregularities detected in respect of a payment card and the use of payment cards and PED's, must be reported immediately to the Corporate Directors.

- **Data Confidentiality for Service Providers / Third Parties:**
  The Authority has a duty of care to its customers and a PCI Compliance obligation to ensure that Service Provider and Third Parties processing or given access to sensitive card data uphold suitable Data and Information Security Practices and Policies and follows the PCI DSS.
  Third party vendors should provide a valid Attestation of Compliance (AOC) as proof of their PCI/DSS compliance.

Commented [CS6]: New addition to policy: point 13

5. Information Security Framework

5.1. Reporting Structure for the Business

5.1.1 Within the Authority the Head of Information Technology is responsible for matters relating to Information Security and PCI compliance.

Commented [CS7]: Was previously Head of Performance and Information: Point 13

5.1.2 This role has responsibility for:

- Overall responsibility for Information Security and related issues.
- Development and maintenance of Information Security Policy and Procedures (including distribution to; and training of, staff in policies).
- Communication and review of Information Security Policy.
- Coordination of PCI Security Audit Tasks.
- Coordination with PCI Accredited Security Auditors (QSA's and ASV's).
- Overall monitoring and analysis of security alerts, and distribution to appropriate Authority personnel.
- Keeping IT staff and management updated on all security related issues.

5.1.3 Venue managers are responsible for ensuring that this policy is adhered to, in particular with regard to:

- Receiving card data
- Transmitting card data
- Processing card transactions/data and
- Storage of card data
- Notification of fraud
- Staff Training and Induction

5.1.4 Staff operating the booking system, specifically processing payment using cards must follow this policy especially for the:

- Checking PED's daily for any form of tampering
- Receiving of card data
- Processing of card transactions/data and
- Storage of card data
- Notification of fraud

5.2. Associated Teams

5.2.1 The following teams are directly involved in the Authority's PCI compliance programme.

Name	Functions (with respect to PCI)	Team Contact Details
Booking Systems	Head of IT	Simon Clark, 01992 709893 sclark@leevalleypark.org.uk
PCI review	Head of IT	Simon Clark, 01992 709893 sclark@leevalleypark.org.uk
Hardware & Network	IT Section	IT Department helpdesk@leevalleypark.org.uk
Internal Audit	Mazars	

Commented [CS8]: Was previously ELMS expert users: Point 13

Commented [CS9]: Was previously Nigel Foxall: Point 13

Commented [CS10]: Was preiously June Darrington: Point 13

5.3. Annual Policy Review

5.3.1 This policy is reviewed and where necessary updated on at least an annual basis. The review process ensures that:

- Perceived threats facing the Authority are identified and consideration included in procedural documentation.
- Any new legal issues are identified that require changes in current policy or practice.
- The Authority meets its compliance obligations to the Payment Card Industry Data Security Standard (the PCI DSS).
- It maintains its relevance to the organisations' current and planned payment card processing operations.
- Any changes to network configuration or new applications are included in Authority's Information Security and IT Usage Policy's.

5.3.2 A formal documented risk assessment process should also be completed annually to identify key business assets (including payment card data stores and supporting networks), and potential threats and vulnerabilities which could impact on the security of those assets.

5.4 Individual Policies

The policies listed below also have a relationship with the current version of the PCI Data Security Standard. Specific policies are listed below:

- IT Usage Policy
- Anti-Fraud, Bribery and Corruption Policy
- Business Continuity Policy
- Data Protection Policy
- Records Management Policy
- Disciplinary Policy
- Anti-Fraud, Corruption and Bribery Policy

6. Policy Communication

6.1 This policy will be circulated to all employees who transact card payments or who have responsibilities for the processing of card payments, and third parties who are authorised to access cardholder data. Changes to, removal of, or the introduction of policies are circulated to relevant parties following their approval by Authority meeting.

7. Training

7.1 Staff are kept aware of policies via the following Authority methods of communication:

- Staff meetings
- Emails, Intranet or Staff Bulletins
- Posters
- Workshops

7.2 Data security awareness training, including authentication procedures and policies, will be conducted for all staff, at least annually to make all personnel aware of the importance of cardholder data security. Users will be made familiar with the password procedures and will be offered training if necessary.

7.3 The Authority shall also ensure that vendors, contractors, and business partners covered by this policy are familiar with its requirements.

7.4 All staff must accept compliance of the Information Security Policy. This ensures that they have read and understood the policy (or changes) and accept any consequences should they fail to adhere to them.

8. Employment Checks

The Authority shall ensure that any new employee directly hired by the Authority who process card payments shall be subjected to pre-employment checks.

9. Policy Breaches

The Authority's Disciplinary Policy and Procedures will be followed where an employee is suspected of breaching this policy and/or any supporting policies or standards. This may include dismissal. Sanctions are covered in more detail in the next section of this Policy.

Sanctions

Where financial impropriety is discovered, the Authority's expectation is that the Police will be involved. Any referral of a case or decision on Police involvement will only be taken by the Corporate Directors.

Any referral to the Police will not prohibit action being taken under the Authority's Disciplinary Policy and Procedures, and it should be noted that an individual could be subject to all, or elements of the following:

- Criminal prosecution;
- Civil Court action to recover money, cost and interest; and
- The Authority's Disciplinary Policy and Procedures.

10. Definitions and References

10.1 **Definitions**

- **IS:** Information Security
- **Payment Card Industry Data Security Standard (PCI DSS):** Currently referenced directly from The PCI Security Standards Council's online resource at https://www.pcisecuritystandards.org
- **AOC:** Attestation of Compliance. The AOC is a form used by merchants and service providers to attest to the results of a PCI DSS assessment

- **PED:** Pin Entry device. A chip and pin device that is used to take card payments.
- **QSA:** Qualified Security Assessor. A third party assessor that conducts onsite PCI audits for Service Providers and Merchants. The QSA is certified annually by The PCI Security Standards Council.
- **ASV:** Approved Scanning Vendor. A third party assessor that conducts quarterly PCI scans against the external card processing environment. The ASV is certified annually by The PCI Security Standards Council.
- **Card Schemes:** Credit Card Associated companies that include Visa, MasterCard, Amex, JCB, Diners.
- **Merchant:** For the purposes of the PCI DSS, a merchant is defined as any entity that accepts payment cards bearing the logos of any of the five members of PCI SSC (American Express, Discover, JCB, MasterCard or Visa) as payment for goods and / or services. Note that a merchant that accepts payment cards as payment for goods and / or services can also be a service provider, if the services sold result in storing, processing, or transmitting cardholder data on behalf of other merchants or service providers. For example, an ISP is a merchant that accepts payment cards for monthly billing, but also is a service provider if it hosts merchants as customers.
- **Service Provider:** Business entity that is not a payment card brand member or a merchant directly involved in the processing, storage, transmission, and switching or transaction data and cardholder information or both. This also includes companies that provide services to merchants, services providers or members that control or could impact the security of cardholder data. Examples include managed service providers that provide managed firewalls, IDS and other services as well as hosting providers and other entities.
- **Acquirer:** Bankcard association member that initiates and maintains relationships with merchants that accept payment cards.
- **Cardholder data:** Full magnetic stripe or the PAN plus any of the following: Cardholder name, Expiration date, Service Code.
- **Cardholder Data Environment: Area** of computer system network that possesses cardholder data or sensitive authentication data and those systems and segments that directly attach or support cardholder processing, storage, or transmission.

Commented [CS11]: Added to report

10.2 References

- Information Security Policy
- Audit Policy
- Business Continuity Policy & Management Procedure
- IT Use Policy
- Information Policy
- Information Policy
- Data Protection Policy
- Records Management Policy
- QMS
- Disciplinary Policy
- Disciplinary Procedure
- Anti-Fraud, Corruption and Bribery Policy

This page is blank