Data Protection and Information Security Policy

This document has been authorised by:

Andrew C Fletcher

Version No.	Date:	Revised By:	Changes Made
2.0			Reviewed & made controlled Document

Contents

Introduction

This Policy document encompasses both the protection of personal data used by ESP Ltd. and all aspects of security surrounding confidential company information. It is distributed to all company employees. All company employees must read this document in its entirety and sign the form confirming they have read and fully understand this policy. This document will be reviewed and updated by Management on an annual basis or when relevant to include newly developed security standards into the policy and re-distributed to all employees and contractors where applicable.

Data Protection Policy

ESP Ltd is committed to a policy of protecting the rights and privacy of individuals (includes learners, staff, clients and others) in accordance with the Data Protection Act.

ESP Ltd needs to process certain information about its staff, clients, learners and other individuals it has dealings with for administrative purposes (e.g. to carry out consultancy, to recruit and pay staff, to administer programmes of study, to record progress, to agree awards, to collect fees, and to comply with legal obligations to funding bodies and government).

To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The policy applies to all staff, clients and learners of ESP Ltd. Any breach of the Data Protection Act 1998 (as amended) or ESP Ltd Data Protection Policy is considered to be an offence and in that event, appropriate disciplinary procedures will apply. As a matter of good practice, other agencies and individuals working with ESP Ltd, and who have access to personal information, will be expected to have read and comply with this policy.

It is expected that departments/sections who deal with external agencies will take responsibility for ensuring that such agencies sign a contract agreeing to abide by this policy.

Background to the Data Protection Act 1998 (as amended)
The Data Protection Act 1998 enhances and broadens the scope of the Data Protection Act 1984. Its purpose is to protect the rights and privacy of living individuals and to ensure that personal data is not processed without their knowledge, and, wherever possible, is processed with their consent.

Definitions
Personal Data
Data relating to a living individual who can be identified from that information or from that data and other information in possession of the data controller. Includes names, addresses, telephone number and e-mail addresses. It also includes expression of opinion about the individual, and of the intentions of the data controller in respect of that individual.

Sensitive Data
Different from ordinary personal data (such as name, address, telephone, e-mail) and relates to racial or ethnic origin, political opinions, religious beliefs, trade union membership, health, sex life, criminal convictions. Sensitive data is subject to much stricter conditions of processing.

Data Controller
Any person (or organisation) who makes decisions with regard to particular personal data, including decisions regarding the purposes for which personal data are processed and the way in which the personal data are processed.

Data Subject
Any living individual who is the subject of personal data held by an organisation.

Processing
Any operation related to organisation, retrieval, disclosure and deletion of data and includes: Obtaining and recording data accessing, altering, adding to, merging or deleting data.

Third Party
Any individual/organisation other than the data subject, the data controller or its agents.

Relevant Filing System
Any paper filing system or other manual filing system, which is structured so that information about an individual is readily accessible. Please note that this is the definition of "Relevant Filing System" in the Act.

Personal data as defined, and covered, by the Act can be held in any format, electronic (including websites and emails), paper-based, photographic etc. from which the individual's information can be readily extracted.

Responsibilities of the Data Protection Act
ESP Ltd as a corporate body is the data controller under the Act.

Compliance with data protection legislation is the responsibility of all members of ESP Ltd who process personal information. Members of ESP Ltd are responsible for ensuring that any personal data supplied to ESP Ltd is accurate and up-to-date.

Data Protection Principles
All processing of personal data must be done in accordance with the eight data protection principles:
1. Personal data shall be processed fairly and lawfully. Those responsible for processing personal data must make reasonable efforts to ensure that data subjects are informed of the identity of the data controller, the purpose(s) of the processing, any disclosures to third parties that are envisaged and an indication of the period for which the data will be kept.
2. Personal data shall be obtained for specific and lawful purposes and not processed in a manner incompatible with those purposes. Data obtained for specified purposes must not be used for a purpose that differs from those.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose for which it is held. Information, which is not strictly necessary for the purpose for which it is obtained, should not be collected. If data is given or obtained which is excessive for the purpose, it should be immediately deleted or destroyed.
4. Personal data shall be accurate and, where necessary, kept up to date. Data, kept for a long time, must be reviewed and updated as necessary. No data should be kept unless it is reasonable to assume accurate. It is the responsibility of individuals to ensure that data held by ESP Ltd is accurate and up-to-date. Completion of an appropriate registration or application form etc will be

taken, as an indication that the data contained therein is accurate. Individuals should notify ESP Ltd of any changes in circumstance to enable personal records to be updated accordingly. It is the responsibility of ESP Ltd to ensure that any notification regarding change of circumstances is noted and acted upon.
5. Personal data shall be kept only for as long as necessary. (See section on Retention and Disposal of Data)
6. Personal data shall be processed in accordance with the rights of data subjects under the Data Protection Act. (See section on Data Subjects Rights)
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of data. (See section on Security of Data)
8. Personal data shall not be transferred to a country or a territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data. Data must not be transferred outside of the European Economic Area (EEA) - the EU Member States together with Iceland, Liechtenstein and Norway - without the explicit consent of the individual.
Members of ESP Ltd should be particularly aware of this when publishing information on the Internet, which can be accessed from anywhere in the globe. This is because transfer includes placing data on a web site that can be accessed from outside the EEA.

Data Subject Rights
Data Subjects have the following rights regarding data processing, and the data that are recorded about them:
- To make subject access requests regarding the nature of information held and to whom it has been disclosed.
- To prevent processing likely to cause damage or distress.
- To prevent processing for purposes of direct marketing.
- To be informed about mechanics of automated decision making process that will significantly affect them.
- Not to have significant decisions that will affect them taken solely by automated process.
- To sue for compensation if they suffer damage by any contravention of the Act.
- To take action to rectify, block, erase or destroy inaccurate data.
- To request the Commissioner to assess whether any provision of the Act has been contravened.

Consent
Wherever possible, personal data or sensitive data should not be obtained, held, used or disclosed unless the individual has given consent. ESP Ltd understands "consent" to mean that the data subject has been fully informed of the intended processing and has signified their agreement, whilst being in a fit state of mind to do so and without pressure being exerted upon them. Consent obtained under duress or on the basis of misleading information will not be a valid basis for processing. There must be some active communication between the parties such as signing a form and the individual must sign the form freely of their own accord. Consent cannot be inferred from non-response to a communication.

For sensitive data, explicit written consent of data subjects must be obtained unless an alternative legitimate basis for processing exists. In most instances consent to process personal and sensitive data is obtained routinely by ESP Ltd (e.g. when a learner signs a registration form or when a new member of staff signs a contract of employment). Any company forms (whether paper-based or

web based) that gather data on an individual should contain a statement explaining what the information is to be used for and to whom it may be disclosed. It is particularly important to obtain specific consent if an individual's data are to be published on the Internet as such data can be accessed from all over the globe.

Therefore, not gaining consent could contravene the eighth data protection principle. If an individual does not consent to certain types of processing (e.g. direct marketing), appropriate action must be taken to ensure that the processing does not take place. If any member of ESP Ltd is in any doubt about these matters, they should consult ESP Ltd Data Protection Officer.

Security of Data
All staff are responsible for ensuring that any personal data (on others), which they hold, are kept securely and that they are not disclosed to any unauthorised third party (see section on Disclosure of Data for more detail). All personal data should be accessible only to those who need to use it.

ESP staff should form a judgement based upon the sensitivity and value of the information in question, but always consider keeping personal data:
- In a lockable room with controlled access, or
- In a locked drawer or filing cabinet, or
- If computerised, password protected, or
- Kept on disks which are themselves kept securely, or
- Kept on a dedicated ESP server.

Personnel files are kept in an electronic folder only accessible to the Directors.

Care should be taken to ensure that PCs and terminals are not visible except to authorised staff and that computer passwords are kept confidential. PC screens should not be left unattended without password protected screen-savers and manual records should not be left where they can be accessed by unauthorised personnel. Care must be taken to ensure that appropriate security measures are in place for the deletion or disposal of personal data. Manual records should be shredded or disposed of as "confidential waste". Hard drives of redundant PCs should be wiped clean before disposal. This policy also applies to staff and learners who process personal data "off-site". Off-site processing presents a potentially greater risk of loss, theft or damage to personal data.

Staff and learners should take particular care when processing personal data at home or in other locations outside of ESP offices. Rights of Access to Data Members of ESP Ltd have the right to access any personal data, which are held by ESP Ltd in electronic format and manual records, which form part of a relevant filing system. This includes the right to inspect confidential personal references received by ESP Ltd about that person. Any individual who wishes to exercise this right should apply in writing to the Data Protection Officer. ESP Ltd reserves the right to charge a fee for data subject access requests (currently £10). Any such request will normally be complied with within 40 days of receipt of the written request and, where appropriate, the fee.

In order to respond efficiently to subject access requests ESP Ltd needs to have in place appropriate records management practices.

Disclosure of Data
ESP Ltd must ensure that personal data is not disclosed to unauthorised third parties which includes family members, friends, government bodies, and in certain circumstances, the Police.

All staff and learners should exercise caution when asked to disclose personal data held on another individual to a third party. For instance, it would usually be deemed appropriate to disclose a colleague's work contact details in response to an enquiry regarding a particular function for which they are responsible. However, it would not usually be appropriate to disclose a colleague's work details to someone who wished to contact them regarding a non-work related matter. The important thing to bear in mind is whether or not disclosure of the information is relevant to, and necessary for, the conduct of company business. Best practice, however, would be to take the contact details of the person making the enquiry and pass them onto the member of ESP Ltd concerned.

This policy determines that personal data may be legitimately disclosed where one of the following conditions apply:
1. The individual has given their consent (e.g. a learner/member of staff has consented to ESP Ltd corresponding with a named third party);
2. Where the disclosure is in the legitimate interests of the institution (e.g. disclosure to staff - personal information can be disclosed to other employees if it is clear that those members of staff require the information to enable them to perform their jobs);
3. Where the institution is legally obliged to disclose the data
4. Where disclosure of data is required for the performance of a contract (e.g. informing a learner of course changes/withdrawal etc).
The Act permits certain disclosures without consent so long as the information is requested for one or more of the following purposes:
- To safeguard national security;
- Prevention or detection of crime including the apprehension or prosecution of offenders;
- Assessment or collection of tax duty;
- Discharge of regulatory functions (includes health, safety and welfare of persons at work);
To prevent serious harm to a third party;
- To protect the vital interests of the individual, this refers to life and death situations.

When members of staff receive enquiries as to whether a named individual is a member of ESP Ltd, the enquirer should be asked why the information is required. If consent for disclosure has not been given and the reason is not one detailed above (i.e. consent not required), the member of staff should decline to comment. Even confirming whether or not an individual is a member of ESP Ltd may constitute an unauthorised disclosure. Unless consent has been obtained from the data subject, information should not be disclosed over the telephone. Instead, the enquirer should be asked to provide documentary evidence to support their request. Ideally a statement from the data subject consenting to disclosure to the third party should accompany the request. As an alternative to disclosing personal data, ESP Ltd may offer to do one of the following:
- Pass a message to the data subject asking them to contact the enquirer;
- Accept a sealed envelope/incoming email message and attempt to forward it to the data subject. Note: the enquirer should be informed that such action will be taken conditionally: i.e. "if the person is a member of ESP Ltd" to avoid confirming their membership of, their presence in or their absence from the institution.

Retention and Disposal of Data
ESP Ltd discourages the retention of personal data for longer than they are required. Considerable amounts of data are collected on current staff and learners. Some data will be kept for longer periods than others.

Clients
In general, records containing information about clients are kept indefinitely and information would typically include correspondence and reports in connection with professional advice.
Information will be either held in physical form or scanned and held electronically if future access is needed. The medium of storage will ensure that it can be easily accessed now and in the future.

Learners
In general, electronic learner records containing information about individual learners are kept indefinitely and information would typically include name and address on entry and completion, programmes taken, examination results, awards obtained. Learner information will be kept electronically.

Staff
In general, electronic staff records containing information about individual members of staff are kept indefinitely and information would typically include name and address, positions held, leaving salary. Other information relating to individual members of staff will be kept for 6 years from the end of employment. Information relating to Income Tax, Statutory Maternity Pay etc will be retained for the statutory time period (between 3 and 6 years). Personal files of individual staff members will be retained in accordance with ESP Ltd policies. Information relating to unsuccessful applicants in connection with recruitment to a post must be kept for 12 months from the interview date. ESP may, if required, keep a record of names of individuals that have applied for, be short-listed, or interviewed, for posts indefinitely. This is to aid management of the recruitment process.

Information will be either held in physical form or scanned and held electronically if future access is needed. The medium of storage will ensure that it can be easily accessed now and in the future.

Disposal of Records
Personal data must be disposed of in a way that protects the rights and privacy of data subjects (e.g., shredding, disposal as confidential waste, secure electronic deletion).

Publication of Company Information
It is recognised that there might be occasions when a member of staff, client, a student, or a lay member of ESP Ltd, requests that their personal details in some of these categories remain confidential or are restricted to internal access. All individuals should be offered an opportunity to opt-out of the publication of the above (and other) data. In such instances, ESP Ltd should comply with the request and ensure that appropriate action is taken.

Direct Marketing
Any department or section that uses personal data for direct marketing purposes must inform data subjects of this at the time of collection of the data. Individuals must be provided with the opportunity to object to the use of their data for direct marketing purposes (e.g. an opt-out box on a form).

Information Security Policy

ESP handles sensitive cardholder information daily. Sensitive Information must have adequate safeguards in place to protect the cardholder data, cardholder privacy, and to ensure compliance with various regulations, along with guarding the future of the organisation.

ESP commits to respecting the privacy of all its customers and to protecting any customer data from outside parties. To this end management are committed to maintaining a secure environment in which to process cardholder information so that we can meet these promises.

Employees handling sensitive cardholder data should ensure:

- Handle Company and cardholder information in a manner that fits with their sensitivity and classification;
- Limit personal use of ESP information and telecommunication systems and ensure it doesn't interfere with your job performance;
- ESP reserves the right to monitor, access, review, audit, copy, store, or delete any electronic communications, equipment, systems and network traffic for any purpose;
- Do not use e-mail, internet and other Company resources to engage in any action that is offensive, threatening, discriminatory, defamatory, slanderous, pornographic, obscene, harassing or illegal;
- Do not disclose personnel information unless authorised;
- Protect sensitive cardholder information;
- Keep passwords and accounts secure;
- Request approval from management prior to establishing any new software or hardware, third party connections, etc.;
- Do not install unauthorised software or hardware, including modems and wireless access unless you have explicit management approval;
- Always leave desks clear of sensitive cardholder data and lock computer screens when unattended;
- Information security incidents must be reported, without delay, to the individual responsible for incident response locally – Please find out who this is.

We each have a responsibility for ensuring our company's systems and data are protected from unauthorised access and improper use. If you are unclear about any of the policies detailed herein you should seek advice and guidance from your line manager.

1. Network Security

A high-level network diagram of the network is maintained and reviewed on a yearly basis. The network diagram provides a high level overview of the cardholder data environment (CDE), which at a minimum shows the connections in and out of the CDE. Critical system components within the CDE, such as POS devices, databases, web servers, etc., and any other necessary payment components, as applicable should also be illustrated.

In addition, ASV should be performed and completed by a PCI SSC Approved Scanning Vendor, where applicable. Evidence of these scans should be maintained for a period of 18 months.

2. Acceptable Use Policy

Management's intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to ESP's established culture of openness, trust and integrity. Management is committed to protecting the employees, partners and ESP from illegal or damaging actions, either knowingly or unknowingly by individuals. ESP will maintain an approved list of technologies and devices and personnel with access to such devices as detailed in Appendix B.

- Employees are responsible for exercising good judgment regarding the reasonableness of personal use.
- Employees should take all necessary steps to prevent unauthorized access to confidential data which includes card holder data.
- Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts.
- All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature.
- All POS and PIN entry devices should be appropriately protected and secured so they cannot be tampered or altered.
- The List of Devices in Appendix B will be regularly updated when devices are modified, added or decommissioned. A stocktake of devices will be regularly performed and devices inspected to identify any potential tampering or substitution of devices.
- Users should be trained in the ability to identify any suspicious behaviour where any tampering or substitution may be performed. Any suspicious behaviour will be reported accordingly.
- Information contained on portable computers is especially vulnerable, special care should be exercised.
- Postings by employees from a Company email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of ESP, unless posting is in the course of business duties.
- Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

3. Protect Stored Data

- All sensitive cardholder data stored and handled by ESP and its employees must be securely protected against unauthorised use at all times. Any sensitive card data that is no longer required by ESP for business reasons must be discarded in a secure and irrecoverable manner.
- If there is no specific need to see the full PAN (Permanent Account Number), it has to be masked when displayed.
- PAN'S which are not protected as stated above should not be sent to the outside network via end user messaging technologies like chats, ICQ messenger etc.,

It is strictly prohibited to store:

1. **The contents of the payment card magnetic stripe (track data) on any media whatsoever.**
2. **The CVV/CVC (the 3 or 4 digit number on the signature panel on the reverse of the payment card) on any media whatsoever.**
3. **The PIN or the encrypted PIN Block under any circumstance.**

4. Information Classification

Data and media containing data must always be labelled to indicate sensitivity level.

- **Confidential data** might include information assets for which there are legal requirements for preventing disclosure or financial penalties for disclosure, or data that would cause severe damage to ESP if disclosed or modified. **Confidential data includes cardholder data**.
- **Internal Use data** might include information that the data owner feels should be protected to prevent unauthorized disclosure.
- **Public data** is information that may be freely disseminated.

5. Access to the Sensitive Cardholder Data

All Access to sensitive cardholder should be controlled and authorised. Any job functions that require access to cardholder data should be clearly defined.

- Any display of the card holder should be restricted at a minimum to the first 6 and the last 4 digits of the cardholder data.
- Access to sensitive cardholder information such as PAN's, personal information and business data is restricted to employees that have a legitimate need to view such information.
- No other employees should have access to this confidential data unless they have a genuine business need.
- If cardholder data is shared with a Service Provider (3rd party) then a list of such Service Providers will be maintained as detailed in Appendix C.
- ESP will ensure a written agreement that includes an acknowledgement is in place that the Service Provider will be responsible for the for the cardholder data that the Service Provider possess.
- ESP will ensure that a there is an established process, including proper due diligence is in place, before engaging with a Service provider.
- ESP will have a process in place to monitor the PCI DSS compliance status of the Service provider.

6. Physical Security

Access to sensitive information in both hard and soft media format must be physically restricted to prevent unauthorised individuals from obtaining sensitive data.

- Media is defined as any printed or handwritten paper, received faxes, floppy disks, back-up tapes, computer hard drive, etc.
- Media containing sensitive cardholder information must be handled and distributed in a secure manner by trusted individuals.
- Visitors must always be escorted by a trusted employee when in areas that hold sensitive cardholder information.
- Procedures must be in place to help all personnel easily distinguish between employees and visitors, especially in areas where cardholder data is accessible. "Employee" refers to full-time and part-time employees, temporary employees and personnel, and consultants who are "resident" on ESP sites. A "visitor" is defined as a vendor, guest of an employee, service personnel, or anyone who needs to physically enter the premises for a short duration, usually not more than one day.
- A list of devices that accept payment card data should be maintained.
- The list should include make, model and location of the device.

- The list should have the serial number or a unique identifier of the device
- The list should be updated when devices are added, removed or relocated
- POS devices surfaces are periodically inspected to detect tampering or substitution.
- Personnel using the devices should be trained and aware of handling the POS devices
- Personnel using the devices should verify the identity of and=y third party personnel claiming to repair or run maintenance tasks on the devices, install new devices or replace devices.
- Personnel using the devices should be trained to report suspicious behaviour and indications of tampering of the devices to the appropriate personnel. ESP sites. A "visitor" is defined as a vendor, guest of an employee, service personnel, or anyone who needs to enter the premises for a short duration, usually not more than one day.
- Strict control is maintained over the external or internal distribution of any media containing card holder data and has to be approved by management
- Strict control is maintained over the storage and accessibility of media
- All computer that store sensitive cardholder data must have a password protected screensaver enabled to prevent unauthorised use.

7. Protect Data in Transit

All sensitive cardholder data must be protected securely if it is to be transported physically or electronically.

- Card holder data (PAN, track data, etc.) must never be sent over the internet via email, instant chat or any other end user technologies.
- If there is a business justification to send cardholder data via email or by any other mode then it should be done after authorization and by using a strong encryption mechanism (i.e. – AES encryption, PGP encryption, IPSEC, etc.).
- The transportation of media containing sensitive cardholder data to another location must be authorised by management, logged and inventoried before leaving the premises. Only secure courier services may be used for the transportation of such media. The status of the shipment should be monitored until it has been delivered to its new location.

8. Disposal of Stored Data

- All data must be securely disposed of when no longer required by ESP, regardless of the media or application type on which it is stored.
- An automatic process must exist to permanently delete on-line data, when no longer required.
- All hard copies of cardholder data must be manually destroyed when no longer required for valid and justified business reasons. A quarterly process must be in place to confirm that all non-electronic cardholder data has been appropriately disposed of in a timely manner.
- ESP will have procedures for the destruction of hardcopy (paper) materials. These will require that all hardcopy materials are crosscut shredded, incinerated or pulped so they cannot be reconstructed.
- ESP will have documented procedures for the destruction of electronic media. These will require:
    - All cardholder data on electronic media must be rendered unrecoverable when deleted e.g. through degaussing or electronically wiped using military grade secure deletion processes or the physical destruction of the media;
    - If secure wipe programs are used, the process must define the industry accepted standards followed for secure deletion.

- All cardholder information awaiting destruction must be held in lockable storage containers clearly marked “To Be Shredded” – access to these containers must be restricted.

9. Security Awareness and Procedures

The policies and procedures outlined below must be incorporated into company practice to maintain a high level of security awareness. The protection of sensitive data demands regular training of all employees and contractors.

- Review handling procedures for sensitive information and hold periodic security awareness meetings to incorporate these procedures into day to day company practice.
- Distribute this security policy document to all company employees to read. It is required that all employees confirm that they understand the content of this security policy document by signing an acknowledgement form (see Appendix A).
- All employees that handle sensitive information will undergo background checks (such as criminal and credit record checks, within the limits of the local law) before they commence their employment with ESP.
- All third parties with access to credit card account numbers are contractually obligated to comply with card association security standards (PCI/DSS).
- Company security policies must be reviewed annually and updated as needed.

10. Credit Card (PCI) Security Incident Response Plan

- ESP PCI Security Incident Response Team (PCI Response Team) is comprised of the Information Security Officer and Merchant Services. ESP PCI security incident response plan is as follows:

    1. Each department must report an incident to the Information Security Officer (preferably) or to another member of the PCI Response Team.
    2. That member of the team receiving the report will advise the PCI Response Team of the incident.
    3. The PCI Response Team will investigate the incident and assist the potentially compromised department in limiting the exposure of cardholder data and in mitigating the risks associated with the incident.
    4. The PCI Response Team will resolve the problem to the satisfaction of all parties involved, including reporting the incident and findings to the appropriate parties (credit card associations, credit card processors, etc.) as necessary.
    5. The PCI Response Team will determine if policies and processes need to be updated to avoid a similar incident in the future, and whether additional safeguards are required in the environment where the incident occurred, or for the institution.

  ESP PCI Security Incident Response Team (or equivalent in your organisation):

  Keith Hampshire - Director
  Oliver Lockwood – Environmental and Energy Consultant
  Judith Dix – Business Development Manager

  Information Security PCI Incident Response Procedures:

- A department that reasonably believes it may have an account breach, or a breach of cardholder information or of systems related to the PCI environment in general, must inform ESP PCI Incident Response Team. After being notified of a compromise, the PCI Response Team, along with other designated staff, will implement the PCI Incident Response Plan to assist and augment departments' response plans.

Incident Response Notification

Escalation Members (or equivalent in your company):

Escalation – First Level:
Judith Dix or Oliver Lockwood

Escalation – Second Level:
Keith Hampshire

External Contacts (as needed)
Merchant Provider Card
Brands
Internet Service Provider (if applicable)
Internet Service Provider of Intruder (if applicable)
Communication Carriers (local and long distance) Business Partners
Insurance Carrier

External Response Team as applicable (CERT Coordination Center 1, etc) Law Enforcement Agencies as applicable inn local jurisdiction

In response to a systems compromise, the PCI Response Team and designees will:

1. Ensure compromised system/s is isolated on/from the network.
2. Gather, review and analyze the logs and related information from various central and local safeguards and security controls
3. Conduct appropriate forensic analysis of compromised system.
4. Contact internal and external departments and entities as appropriate.
5. Make forensic and log analysis available to appropriate law enforcement or card industry security personnel, as required.
6. Assist law enforcement and card industry security personnel in investigative processes, including in prosecutions.

The credit card companies have individually specific requirements that the Response Team must address in reporting suspected or confirmed breaches of cardholder data. See below for these requirements.

Incident Response notifications to various card schemes

1. In the event of a suspected security breach, alert the information security officer or your line manager immediately.
2. The security officer will carry out an initial investigation of the suspected security breach.
3. Upon confirmation that a security breach has occurred, the security officer will alert management and begin informing all relevant parties that may be affected by the compromise.

VISA Steps

If the data security compromise involves credit card account numbers, implement the following procedure:

- Shut down any systems or processes involved in the breach to limit the extent, and prevent further exposure.
- Alert all affected parties and authorities such as the Merchant Bank (your Bank), Visa Fraud Control, and the law enforcement.
- Provide details of all compromised or potentially compromised card numbers to Visa Fraud Control within 24 hrs.
- For more Information visit: http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp_if_ compromised.html

Visa Incident Report Template

This report must be provided to VISA within 14 days after initial report of incident to VISA. The following report content and standards must be followed when completing the incident report. Incident report must be securely distributed to VISA and Merchant Bank. Visa will classify the report as "VISA Secret"*.

I. Executive Summary
   a. Include overview of the incident
   b. Include RISK Level(High, Medium, Low)

   c. Determine if compromise has been contained
II. Background
III. Initial Analysis
IV. Investigative Procedures
   a. Include forensic tools used during investigation
V. Findings
   a. Number of accounts at risk, identify those stores and compromised
   b. Type of account information at risk
   c. Identify ALL systems analyzed. Include the following:
      - Domain Name System (DNS) names
      - Internet Protocol (IP) addresses
      - Operating System (OS) version
      - Function of system(s)
   d. Identify ALL compromised systems. Include the following:
      - DNS names
      - IP addresses
      - OS version
      - Function of System(s)
   e. Timeframe of compromise
   f. Any data exported by intruder
   g. Establish how and source of compromise
   h. Check all potential database locations to ensure that no CVV2, Track 1 or Track 2 data is stored anywhere, whether encrypted or unencrypted (e.g., duplicate or backup tables or databases, databases used in development, stage or testing environments, data on software engineers' machines, etc.)
   i. If applicable, review VisaNet endpoint security and determine risk
VI. Compromised Entity Action
VII. Recommendations
VIII. Contact(s) at entity and security assessor performing investigation

*This classification applies to the most sensitive business information, which is intended for use within VISA. Its unauthorized disclosure could seriously and adversely impact VISA, its employees, member banks, business partners, and/or the Brand.

MasterCard Steps:

I. Within 24 hours of an account compromise event, notify the MasterCard Compromised Account Team via phone at 1-636-722-4100.
II. Provide a detailed written statement of fact about the account compromise (including the contributing circumstances) via secured e-mail to compromised_account_team@mastercard.com.
III. Provide the MasterCard Merchant Fraud Control Department with a complete list of all known compromised account numbers.
IV. Within 72 hours of knowledge of a suspected account compromise, engage the services of a data security firm acceptable to MasterCard to assess the vulnerability of the compromised data and related systems (such as a detailed forensics evaluation).
V. Provide weekly written status reports to MasterCard, addressing open questions and issues until the audit is complete to the satisfaction of MasterCard.
VI. Promptly furnish updated lists of potential or known compromised account numbers, additional documentation, and other information that MasterCard may request.
VII. Provide finding of all audits and investigations to the MasterCard Merchant Fraud Control

department within the required time frame and continue to address any outstanding exposure or recommendation until resolved to the satisfaction of MasterCard.

Once MasterCard obtains the details of the account data compromise and the list of compromised account numbers, MasterCard will:

1. Identify the issuers of the accounts that were suspected to have been compromised and group all known accounts under the respective parent member IDs.

2. Distribute the account number data to its respective issuers.

Employees of ESP will be expected to report to the security officer for any security related issues. The role of the security officer is to effectively communicate all security policies and procedures to employees within ESP and contractors. In addition to this, the security officer will oversee the scheduling of security training sessions, monitor and enforce the security policies outlined in both this document and at the training sessions and finally, oversee the implantation of the incident response plan in the event of a sensitive data compromise.

Discover Card Steps

I. Within 24 hours of an account compromise event, notify Discover Fraud Prevention at (800) 347-3102
II. Prepare a detailed written statement of fact about the account compromise including the contributing circumstances
III. Prepare a list of all known compromised account numbers
IV. Obtain additional specific requirements from Discover Card

American Express Steps

I. Within 24 hours of an account compromise event, notify American Express Merchant Services at (800) 528-5200 in the U.S.
II. Prepare a detailed written statement of fact about the account compromise including the contributing circumstances
III. Prepare a list of all known compromised account numbers Obtain additional specific requirements from American Express

11. Transfer of Sensitive Information Policy

- All third-party companies providing critical services to ESP must provide an agreed Service Level Agreement.
- All third-party companies providing hosting facilities must comply with ESP's Physical Security and Access Control Policy.
- All third-party companies which have access to Card Holder information must

    1. Adhere to the PCI DSS security requirements.
    2. Acknowledge their responsibility for securing the Card Holder data.

3. Acknowledge that the Card Holder data must only be used for assisting the completion of a transaction, supporting a loyalty program, providing a fraud control service or for uses specifically required by law.
4. Have appropriate provisions for business continuity in the event of a major disruption, disaster or failure.
5. Provide full cooperation and access to conduct a thorough security review after a security intrusion by a Payment Card industry representative, or a Payment Card industry approved third party.

12. User Access Management

- Access to ESP is controlled through a formal user registration process beginning with a formal notification from HR or from a line manager.
- Each user is identified by a unique user ID so that users can be linked to and made responsible for their actions. The use of group IDs is only permitted where they are suitable for the work carried out.
- There is a standard level of access; other services can be accessed when specifically authorized by HR/line management.
- The job function of the user decides the level of access the employee has to cardholder data
- A request for service must be made in writing (email or hard copy) by the newcomer's line manager or by HR. The request is free format, but must state:

  Name of person making request;
  Job title of the newcomers and workgroup;
  Start date;
  Services required (default services are: MS Outlook, MS Office and Internet access).

- Each user will be given a copy of their new user form to provide a written statement of their access rights, signed by an IT representative after their induction procedure. The user signs the form indicating that they understand the conditions of access.
- Access to all ESP systems is provided by IT and can only be started after proper procedures are completed.

- As soon as an individual leaves ESP employment, all his/her system logons must be immediately revoked.
- As part of the employee termination process HR (or line managers in the case of contractors) will inform IT operations of all leavers and their date of leaving.

13. Access Control Policy

- Access Control systems are in place to protect the interests of all users of ESP computer systems by providing a safe, secure and readily accessible environment in which to work.
- ESP will provide all employees and other users with the information they need to carry out their responsibilities in an as effective and efficient manner as possible.
- Generic or group IDs shall not normally be permitted, but may be granted under exceptional circumstances if sufficient other controls on access are in place.

- The allocation of privilege rights (e.g. local administrator, domain administrator, super-user, root access) shall be restricted and controlled, and authorization provided jointly by the system owner and IT Services. Technical teams shall guard against issuing privilege rights to entire teams to prevent loss of confidentiality.
- Access rights will be accorded following the principles of least privilege and need to know.
- Every user should attempt to maintain the security of data at its classified level even if technical security mechanisms fail or are absent.
- Users electing to place information on digital media or storage devices or maintaining a separate database must only do so where such an action is in accord with the data's classification.
- Users are obligated to report instances of non-compliance to ESP CISO.
- Access to ESP IT resources and services will be given through the provision of a unique Active Directory account and complex password.
- No access to any ESP IT resources and services will be provided without prior authentication and authorization of a user's ESP Windows Active Directory account.
- Password issuing, strength requirements, changing and control will be managed through formal processes. Password length, complexity and expiration times will be controlled through Windows Active Directory Group Policy Objects.
- Access to Confidential, Restricted and Protected information will be limited to authorised persons whose job responsibilities require it, as determined by the data owner or their designated representative. Requests for access permission to be granted, changed or revoked must be made in writing.
- Users are expected to become familiar with and abide by ESP policies, standards and guidelines for appropriate and acceptable usage of the networks and systems.
- Access for remote users shall be subject to authorization by IT Services and be provided in accordance with the Remote Access Policy and the Information Security Policy. No uncontrolled external access shall be permitted to any network device or networked system.
- Access to data is variously and appropriately controlled according to the data classification levels described in the Information Security Management Policy.
- Access control methods include logon access rights, Windows share and NTFS permissions, user account privileges, server and workstation access rights, firewall permissions, IIS intranet/extranet authentication rights, SQL database rights, isolated networks and other methods as necessary.
- A formal process shall be conducted at regular intervals by system owners and data owners in conjunction with IT Services to review users' access rights. The review shall be logged and IT Services shall sign off the review to give authority for users' continued access rights.

Appendix A – Agreement to Comply Form – Agreement to Comply With Information Security Policies

JUDITH DIX

_____
Employee Name (printed)

Business Development
Department

I agree to take all reasonable precautions to assure that company internal information, or information that has been entrusted to ESP by third parties such as customers, will not be disclosed to unauthorised persons. At the end of my employment or contract with ESP, I agree to return all information to which I have had access as a result of my position. I understand that I am not authorised to use sensitive information for my own purposes, nor am I at liberty to provide this information to third parties without the express written consent of the internal manager who is the designated information owner.
I have access to a copy of the Information Security Policies, I have read and understand these policies, and I understand how it impacts my job. As a condition of continued employment, I agree to abide by the policies and other requirements found in ESP security policy. I understand that non-compliance will be cause for disciplinary action up to and including dismissal, and perhaps criminal and/or civil penalties.
I also agree to promptly report all violations or suspected violations of information security policies to the designated security officer.

_____
Employee Signature

23/04/2018

_____
Date

Appendix B – List of Devices

Asset/Device Name	Description	Owner/Approved User	Location
Not Applicable			

Appendix C – List of Service Providers

Name of Service Provider	Contact Details	Services Provided	PCI DSS Compliant	PCI DSS Validation Date
Netscan	02088168812	Web Hosting	Yes	Unsure – Handled by WorldPay