# Essex County Council

# Information Policy Requirements for Contractors

| | |
|---|---|
| Title | Essex County Council Information Policy Requirements for Contractors |
| Author/Owner | Information Governance Team |
| Status | APPROVED |
| Version | 7.0 |
| Date Approved | 14/09/2018 |
| Security Classification | OFFICIAL |

| Version | Created/ Reviewed by | Date | Details |
|---|---|---|---|
| 1.0 | Information Governance | 28/06/2018 | First published version |
| 2.0 | Information Governance | 14/09/2018 | ECC protective measures added |
| 3.0 | Information Governance | 04/02/2021 | ECC technical protective measures revised and enhanced |
| 4.0 | Information Governance | 20/04/2021 | Glossary Terms added to and review of document undertaken |
| 5.0 | Information Governance | 27/06/2022 | Review of Document |
| 6.0 | Information Governance | 10/07/2023 | Technical Services requirements section updated |
| 7.0 | Information Governance | 05/03/2024 | Supplier Assurance Standards section updated by TS |

## Introduction

Where information and personal data are processed by a Contractor on behalf of Essex County Council (ECC), ECC retains responsibility to ensure that it is processed according to the law and to ensure efficient service delivery. To achieve this, the controls within this policy must be in place and the requirements met; managed by Contractor Parties and Staff and monitored by ECC.

This policy is applicable where there is a contract in place with ECC which includes the accompanying Information Handling Schedule and Data Processing Schedule.

The Contractor must ensure that anyone processing ECC data, defined in the contract as a Contractor Party or Staff, is aware of these policy requirements.

## Information Breach Process

Any Information Breach or breach of the Information Handling Schedule/Agreement and/or this policy will be investigated and may result in contractual action.

The Contractor must have processes in place to capture and manage Information Breaches.

Where regular performance reporting is required by ECC, the Contractor must provide Information Breach statistical data. Detailed Information Breach evidence must be supplied on demand.

The Contractor must report all Information Breaches immediately to ECC's Information Governance (IG) Team and Procurement Team for formal notification as soon as they are identified and must update the IG Team on the investigation progress and final resolution as directed.

- In the first instance, an email to notify ECC of the breach is to be sent to the following email addresses, without any personal data or commercially sensitive information:
    - IGTeam@essex.gov.uk
    - commercial.team@essex.gov.uk
- Following this, ECC will respond via secure email for further detail as required.

Criminal incidents must be reported to law enforcement agencies.

## Privacy Management

The Contractor must take appropriate steps to safeguard the privacy of data subjects and only process personal data on behalf of ECC in line with the Data Processing Schedule.

The Contractor must comply with the relevant privacy notice for the service.

Where the Contractor proposes to create a new or amend an existing system/process affecting the processing of personal data, the proposal must be referred to ECC's IG Team for guidance on whether a Data Protection Impact Assessment (DPIA) needs to be undertaken.

## Physical Security

### *Use of ECC Premises:*

Where the Contractor is/are based in or utilise ECC's premises, the Contractor must ensure that they comply with ECC ID Cards and Building Security Policy.

The Contractor must supply data on request of those employees who it approves to hold ECC ID Cards. Such data must be sufficient to identify individual employees to manage their card entitlement.

The Contractor must advise ECC immediately of any individual leaving their organisation so that access to our premises can be terminated and any third party user accounts that they hold can be deleted.

### *Use of Non-ECC Premises:*

The Contractor must ensure that premises (and dedicated areas where ECC data is stored within premises including any Cloud Services) are protected against unauthorised entry and theft of or damage to ECC data.

Access to building entry keys and keys which secure rooms or storage equipment must be controlled and custody recorded.

The Contractor must regularly change access codes and/or relevant codes immediately when an individual no longer as any requirement to gain access to the premises.

## Data Subject Rights:

The Contractor shall assist ECC in safeguarding the relevant applicable legal rights of the Data Subject as identified in the privacy notice for the service being delivered.

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure (Right to be forgotten)
- The right to restrict processing
- The right to data portability
- The right to object
- The right to object to Direct Marketing
- Rights related to automated decision making and profiling

If the Contractor receives a Data Subject Rights request, they are to immediately notify ECC's Data Protection Officer.

- In the first instance, an email to notify ECC of the request is to be sent, without any personal data to the below address:
    - DPO@essex.gov.uk

- Following this, ECC will respond via secure email for further detail as required.

If ECC contacts the Contractor with a Data Subject Right request, the Contractor shall action the request within 10 working days of receipt of instruction by ECC, unless an extension is agreed.

## Security Classification

ECC complies with the Government Security Classifications Policy: https://www.gov.uk/government/publications/government-security-classifications

Contractors must comply with this classification policy when processing information on behalf of ECC. All information processed by or on behalf of ECC falls within the category of 'OFFICIAL', with some data falling within the sub section 'OFFICIAL-SENSITIVE'.

## Retention and destruction

ECC data must be retained in line with ECC's Corporate Retention Schedule and destroyed securely with the explicit approval of ECC or by standing agreement with ECC which provides for the Contractor to destroy data once agreed criteria has been met.

Where the Contractor destroys data, this activity must be evidenced by recording the criteria for destruction, approval, date and method of the destruction activity and certification of completion and follow the requirements.

The ECC Corporate Retention Schedule is available here

Where the Contractor has the authority to dispose of ECC data in accordance with the ECC Corporate Retention Schedule or by virtue of any additional agreement, the data must be disposed of by methods appropriate to its security classification.

Destruction processes must ensure that the data is kept secure from disclosure to unauthorised persons until and during destruction, and that the data cannot be reconstituted after the destruction process.

## Equipment Security

This includes any device (desktop, laptop, tablet, mobile phone) used to access ECC data, and the following must be assured:

- Contractors must ensure that all relevant security solutions are enabled on portable equipment, such as pin codes and password access
- Users must not access ECC data on devices that do not have relevant protective measures in place
- Equipment must be switched off or 'locked' after an appropriate period of inactivity and require a password to re-access
- When stored in office space, laptops must be secured with lock devices or in lockable storage to prevent theft
- When devices accessing ECC data are used in users' homes, they must be protected from use by any unauthorised persons and must be stored out of sight when not in use to prevent theft
- When laptops are being transported they must not be left unattended, kept out of sight

when not being used, and (where available) stored in secure transportation equipment such as a code-lock case

- Any individual for whom the Contractor is responsible (and who accesses ECC data) must return devices to the Contractor when their role requiring access to the ECC data ends, or their role no longer entitles them to such equipment
- Devices accessing ECC data should not be taken outside of the European Economic Area (EEA) unless a) there is a strong business need approved by the Contractor's governance processes and by ECC, and b) there are sufficient security controls in place on the device to allow its use without exposing ECC data to malicious activity or unauthorised disclosure.
- Users must report lost or stolen equipment to the Contractor immediately and where any ECC data is at risk the loss must be handled as an Information Breach

**Asset Management**

- A register must be maintained of the physical hardware items (assets) which the Contractor uses to access ECC data. Assets must be uniquely identified, have an identified custodian (who will be accountable for the use and safe keeping of the asset) and have up to date details of versions of relevant anti-malware and encryption solutions installed
    - The register must be promptly updated for new and decommissioned items, change of custodian, and change of anti-malware and encryption solutions, so that it remains current
- Paper records must be stored in lockable equipment or dedicated rooms with access to keys or codes managed
    - Such accommodation must include appropriate protection against fire and flood
- Paper filing systems must be well maintained, using clear, logical, and consistent referencing, and kept in good condition to support identification and retrieval
- When paper records are being transported they must not be left unattended, must be kept out of sight when not being used, and (where available) stored in secure transportation equipment such as a code-lock case
    - Paper records that are being transported must be kept separate from electronic equipment
- Where paper records contain Official-Sensitive ECC data, removing them from storage must be a recorded activity
- Where paper records are in the custody of a third-party storage provider, a Sub-Processor Arrangement must be in place as per the Information Handling Schedule. The Contractor must ensure that detailed inventories are maintained to ensure the effective identification and retrieval of individual files and that storage and transfer processes offer appropriate levels of security to the security classification of the data.
- The Contractor must maintain a current and accurate knowledge of the ECC data it holds in all formats, on what systems it resides and the physical locations in which those systems are stored.
    - Internal ownership must be established with owners aware of their responsibilities under these requirements.

**Removable media**

- Removable media refers to USB drives, CDs, DVDs, secure digital cards, and devices which permit the storage of data on memory cards, but also refers to hard copy such as paper files.
- Removable media should only be used where there is a clear business need.
- Where the Contractor allows for the use of removable media, the Contractor must encrypt to an appropriate level any device storing digital ECC data that would cause damage or distress to individuals, or reputational damage to the Contractor or ECC if it were lost or stolen.
- The Contractor must ensure that the level of security applied to office-located devices is applied to ECC data on removable media being used away from the office.
- Personal data must only be held on removable digital media for transfer purposes and must be securely deleted once copied to its formal storage location.
- The Contractor must maintain a removable media policy for the storage of information that:
    - Controls access to, and the use of removal media
    - Limits the type of media that can be used
    - Defines user permissions, and the information types that can be stored
    - Ensures that all clients and hosts automatically scan removable media for malware before first use, and any subsequent data transfer takes place
- Where removable media is to be reused or destroyed, appropriate steps should be taken to ensure that previously stored information will not be accessible.

**Email**

- The Contractor must ensure that employees are aware of the importance of correctly addressing emails (as with hard-copy mail), to reduce instances of loss of ECC data or it being received by an incorrect recipient.
- Contractor must ensure that no employees set up auto forwarding within their emails which would result in all emails being redirected to another individual, this could result in information being received by an unintended audience.
- Where the Contractor needs to send Official-Sensitive ECC data by email (or post), the Contractor must ensure that employees have been authorised to do so and follow the security classification requirements.
- Where secure email facilities are not available, emails must be sent with the Official-Sensitive ECC data in a password protected attachment, with the recipient informed of the password via an alternative method to email.
- Where the Contractor's employees send ECC data to the incorrect recipient, the Contractor must manage this as an Information Breach and ensure the data is recovered. If the data is personal this must be reported to ECC in line with the Information Breach Process in order to consider further actions in regards to the data subject and supervisory authority.

## Secure Email

- Where the Contractor has access to secure government systems such as PSN, CJSM etc. and the recipient can receive securely, then these facilities must always be used to send Official-Sensitive ECC data.
- Where the Contractor has access to accredited secure email tools then these facilities must always be used to send Official-Sensitive ECC data.

## Information Management

### Accessibility

- The Contractor must ensure that ECC data held on its systems is maintained in such a way that those who have the rights to access can:
    - Do so promptly
    - Easily identify and locate information
    - Easily establish the most current and complete version
    - Understand who they may share it with and under what circumstances
    - Easily establish audit trails of services delivered and related authorisations, for use in ECC performance monitoring and internal or external auditing.

## Data Quality

The Contractor must provide data quality processes to support effective service delivery and decision making. Quality data has the following characteristics:

- **Accurate:** It must provide a true account of what it is intended to represent to enable informed decisions to be made. Limitations in the level of accuracy must be stated to help appropriate interpretation of resulting information. Maintaining the accuracy of Personal Data is a requirement of Data Protection Legislation
- **Valid:** Data must appropriately reflect what it is intended to measure or report
- **Reliable:** Data must be consistently calculated, recorded, analysed and reported over time in a way that provides a meaningful reflection of the situation to give managers and stakeholders confidence that progress towards targets reflects real changes rather than variations in data collection approaches
- **Timely:** Data must be available frequently and captured promptly enough to be of value
- **Relevant:** Data must be defined, selected, collected, recorded and analysed with the intended use and audience in mind so that it is fit for purpose and adds value. Consideration should be given to using anonymisation or psuedonymisation techniques at all times to comply with the Data Minimisation principle in Data Protection Legislation
- **Complete:** Data must be complete and comprehensive to ensure it provides a full picture of a current situation, and caveated where it is incomplete

The Contractor must support regular reviews, sample auditing, and provide feedback to achieve and maintain an acceptable standard of data quality.

## Acceptable Personal Use

Where information facilities (such as email) can be used to access ECC data, but can also be used for personal purposes, the Contractor must:

- Have a clear policy on what constitutes acceptable personal use,
- Communicate this to all individuals who access ECC data

Where such use is permitted, the Contractor must ensure that activity can be evidenced in the event of ECC data being misused, resulting in an information breach.

## Use of ECC's SharePoint/Microsoft Teams Collaboration Sites/Federated online services

Where the Contractor is granted access to SharePoint/Microsoft Teams collaboration sites hosted by ECC which allow the sharing and editing of information of mutual interest, the Contractor must ensure that they adhere to the SharePoint Collaboration Site Guidelines.

This would also include the use of federated online messaging facilities, where the Contractor has federated online messaging functionality with ECC, the facility must not be used for the transfer of Official-Sensitive data and must not be the medium used to communicate and record contract decisions and actions. The Contractor must also evidence appropriate policies and practices in its use of online messaging facilities for ECC to approve and maintain federation.

## Caldicott Principles

The Contractor must observe the Caldicott Principles when processing health and/or social care data, which are set out below:

- **1. Justify the purpose(s)** - Every proposed use or transfer of personal confidential data within or from an organisation should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed, by an appropriate guardian.
- **2. Don't use personal confidential data unless it is absolutely necessary** - Personal confidential data items should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).
- **3. Use the minimum necessary personal confidential data** - Where use of personal confidential data is considered to be essential, the inclusion of each discrete item of data should be considered and justified so that the minimum amount of personal confidential data is transferred or accessible as is necessary for a given function.
- **4. Access to personal confidential data should be on a strict need-to-know basis** - Only those individuals who need access to personal confidential data should have access to it, and they should only have access to the data items that they need to see. This may mean introducing access controls or splitting data flows where one data flow is used for several purposes.
- **5. Everyone with access to personal confidential data should be aware of their responsibilities** - Action should be taken to ensure that those handling personal confidential data — both clinical and non-clinical employees — are made fully aware of their responsibilities and obligations to respect patient confidentiality.
- **6. Comply with the law** - Every use of personal confidential data must be lawful. Someone in each organisation handling personal confidential data should be responsible for ensuring that the organisation complies with legal requirements.
- **7. The duty to share information can be as important as the duty to protect patient confidentiality** - Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles. They should be supported by the policies of their employers, regulators, and professional bodies.
- **8. Inform patients and service users about how their confidential information is used –** A range of steps should be taken to ensure no surprises for patients and service users, so they can have clear expectations about how and why their confidential information is used, and what choices they have about this. These steps will vary depending on the use: as a minimum, this should include providing accessible, relevant, and appropriate information – in some cases, greater engagement will be required.

## Protective Measures

ECC requires its Contractors to have relevant technical and organisational measures (protective measures) in place to protect ECC's data. As well as the supplier of a solution/service, this also applies to any sub-contractors/sub-processors the Contractor uses (or intends to use) to provide the solution/service – any that will access, process, store or communicate information, or provide IT infrastructure components. It's the Contractor's responsibility to check that all these parties have relevant protective measures in place.

ECC requires Contractors follow best practice guidance and have in place (and be able to provide evidence it if requested) 'protective measures' in line with the following:

- National Cyber Security Centre (NCSC) 's:
  - 10 Steps To Cyber Security publication
  - Cyber Essentials scheme requirements
  - Cloud Security Principles
  - Other guidance provided
- The Information Commissioner's Office (ICO) Practical guide to IT Security

These measures must result in a minimum of the following outcomes:

- Appropriate protection from malware (e.g. Viruses, Worms, Ransomware etc.)
- Securely configured and maintained systems
- Effective account provisioning and management, and controlled privileged access
- Use of software that is supported, kept up-to-date and secured with regular security updates
- Use of networks that are protected from external and internal attacks
- Logging and monitoring of appropriate device, system, and network events
- Third-party services used include appropriate technical and organisational protective measures.
- Management of risks to the organisation and information, including those posed by mobile working and remote access to systems.
- Staff effectively supported using the right tools, education, and awareness
- Effective incident management policies and processes.

Some readers of this policy may not be familiar with some of the terms used in the examples, Appendix C - Glossary of Terms has been provided to assist you. The examples are current at the time of writing this policy, but please check the links above to ensure you adhere to the latest NCSC and ICO guidance.

Where certification or accreditation is held by the Contractor that demonstrates the Protective Measures that are in place (such as a Cyber Essentials 'Plus' Certificate), this should be provided to ECC as soon as possible.

# ECC Supplier Assurance Standards

## Basic Assurance Level

As a minimum for non-technical service offerings, ECC requires that technical protective measures are implemented in line with the following standards:

| | |
|---|---|
| National Cyber Security Centre<br>Small Business Guide: Cyber Security<br>Cyber Essentials | https://www.ncsc.gov.uk/<br><br>https://www.ncsc.gov.uk/files/NCSC_A5_Small_Business_Guide_v4_OCT20.pdf<br>https://www.ncsc.gov.uk/cyberessentials/overview |
| Information Commissioner's Office<br>A practical guide to IT security | https://ico.org.uk/<br>https://ico.org.uk/media/for-organisations/documents/1575/it_security_practical_guide.pdf |

## Enhanced Assurance Level

When a contractor is supplying technology services (types listed below) to ECC they must ensure the service is delivered in line with the required standards.

## Cloud – Lightweight Software as a Service (SaaS)

This approach is intended for uses by any organisation where the service will **not** be holding or processing **sensitive** data.

Method of providing software to users. SaaS users subscribe to an application rather than purchasing it once and installing it. Users can log into a service from any compatible device over the Internet. The application runs in cloud servers. SaaS services are entirely managed by the vendor.

| Service Type | Required standard | |
|---|---|---|
| Lightweight Software as a Service (SaaS) | NCSC SaaS Cloud Security Principles | https://www.ncsc.gov.uk/collection/saas-security/saas-security-principles |

**The supplier must be able to evidence the following:**

- Supplier must provide a clear assertion that NCSC SaaS Security guidance is met and provide independent verification as evidence that the security controls are effectively implemented.
- Independent verification can be a penetration test report or a certification that meets the required technical controls within the guidance.

## Cloud – Software as a Service (SaaS)

If offering a SaaS service for more sensitive workloads (such as processing large amounts of personal data, commercially sensitive information, or as part of a larger more trusted system), assertion and evidence that the full 14 cloud security principles are covered must be provided.

Note that the lightweight framework does **not** directly consider some potentially important issues regarding cloud security and risk management.

| Service Type | Required standard | |
|---|---|---|
| Software as a Service (SaaS) | NCSC SaaS Cloud Security Principles | https://www.ncsc.gov.uk/collection/cloud/the-cloud-security-principles |

**The supplier must be able to evidence the following:**

- Supplier must provide a clear assertion that NCSC Cloud Security Principles is met and provide independent verification as evidence that the security controls are effectively implemented.
- Independent verification can be a penetration test report or a certification that meets the required technical controls within the guidance.

## Cloud – Infrastructure/Platform as a Service (IaaS/PaaS)

Infrastructure as a Service - vendor hosts infrastructure on behalf of a customer in "the cloud", i.e., in various data-centres. Customers access cloud infrastructure by Internet and use it to build/host web-apps, store data, run business logic or other tasks that could be done on traditional on-prem infrastructure, often with more flexibility.

Platform as a Service - is the next layer up from IaaS in the cloud computing service model. It provides developers with a platform for building applications and includes dev tools, middleware, O/S systems, DB management and infrastructure.

| Service Type | Required standard | |
|---|---|---|
| Cloud Service Provider (IaaS/PaaS) | NCSC Cloud Security Principles | https://www.ncsc.gov.uk/collection/cloud-security/implementing-the-cloud-security-principles |
| | ISO 27017 | https://www.iso.org/standard/43757.html |
| | CSA Cloud Control Matrix | https://cloudsecurityalliance.org/research/cloud-controls-matrix/ |

**The supplier must be able to evidence any of the following:**

- certified to ISO 27017.
- The supplier adheres to the expectations of ISO 27017 and is working towards accreditation. Can provide independent verification as evidence that the security controls are effectively implemented.
- The supplier must assert and evidence that they adhere to the Cloud Security Alliance (CSA) Cloud Control Matrix framework.
- Supplier asserts how they meet the NCSC Cloud Security Principles and provides independent verification as evidence that the security controls are implemented.

## Hosted Service

This service model is offered by a vendor who owns and maintains physical servers in a private location.

| Service Type | Required standard |
|---|---|

| | | |
|---|---|---|
| Hosted Service | Cyber Essentials Plus | https://iasme.co.uk/cyber-essentials/cyber-essentials-plus-find-out-more/ |
| | NCSC: 10 Steps to Cyber Security | https://www.ncsc.gov.uk/collection/10-steps |

**The supplier must be able to evidence any of the following:**

- Supplier is certified with Cyber Essentials Plus, which includes a technical audit of the controls that have been implemented. Certificate must be provided as evidence.
- The supplier must be certified with Cyber Essentials and provide independent verification as evidence that the Cyber Essentials security controls in their assertion are effectively implemented.
- The supplier must give clear assurance that they meet all controls within the NCSC 10 steps to Cyber Security requirement and provide independent verification as evidence that the security controls are effectively implemented.

## Payment Card Processing

The Payment Card Industry Data Security Standard (PCI DSS) is a set of security standards designed to ensure ALL companies that accept, process, store or transmit credit card information maintain a secure environment.

| Service Type | Required standard | |
|---|---|---|
| Payment Card Processing | PCI-DSS | https://www.pcisecuritystandards.org/document_library |

**Service offering must be compliant** with current PCI-DSS certification level and independent verification provided to show that that the security controls are effectively implemented.

## Appendix A – SharePoint Collaboration Site Guidelines

Where the Contractor is granted access to SharePoint sites hosted by ECC which allow the sharing of and collaboration on information of mutual interest, the Contractor must ensure that:

- There is a register maintained of employees who have access to sites, and that the access is always necessary and therefore valid and available for auditing by ECC.
- Where employees leave the organisation, or when they change to a role which no longer requires access or when access credentials have been compromised, the Contractor must inform the relevant ECC SharePoint Site Manager to allow accounts and permissions to be managed accordingly
- Those with rights to add or edit documents must comply with the ECC Site Owner's requirements over assigning document metadata, titling conventions and correct document library storage
- Copies of documents containing ECC data available on the sites are not stored outside of the site or shared/ disclosed beyond the permissions group of the site without the permission of the Site Owner.
- Where a site is accessible by a number of Contractors, Suppliers and Partners, any information which a Contractor does not wish to be available to anyone other than ECC and its own employees must be stored in a document library for the appropriate audience, provided by ECC.
- Its employees are aware that all information on the site is accessible to ECC and is information held by ECC for the purposes of the Freedom of Information Act (2000), with the Contractor offered the opportunity to present prejudice and public interest cases prior to disclosure.
- Where the Contractor is a Public Authority under Schedule 1 of the Freedom of Information Act (2000), its employees must be aware that disclosure of any ECC data stored on a site in response to requests for information must be referred to ECC for clarification on whether the data is held for the purposes of the Act, and if so, for consideration of valid exemptions.

## Appendix B - ECC ID Cards and Building Security Policy

- You must not allow anyone to follow you through a security door (tailgating) without clearly displaying a valid ID Card.
- You must carry your ECC ID Card or Visitor pass and display it at all times when in ECC buildings, or to prove to a member of the public or staff of another organisation that you are representing ECC on official business. Otherwise, when outside of ECC premises you should keep your pass hidden to ensure personal security.
- You must not share your ECC ID Card with anyone or share door codes or keys with unauthorised people.
- If you find a lost ECC ID Card, you must hand it in to the nearest reception or security office.
- If you lose your pass or it is stolen, you must report it to Mitie Security.
- All leavers must hand their pass to their line-manager as part of the leavers' process.
- You must supervise all visitors that you allow into a secure work area at all times until they leave.
- You must ensure door codes and security alarms are changed regularly.
- All employees must ensure offices are secure if they are the last person to leave at the end of the working day.
- Mitie security must perform regular checks of staff compliance with this policy.
- All employees/ agency workers/ consultants/ elected members must assist Mitie Security with checks of compliance with this policy.
- Any ID Card which provides access to ECC buildings, or visibly identifies a person as being employed by ECC (or by an employer in partnership or under contract to ECC), or visibly identifies that a person has been approved by ECC to carry out a service, must be provided and recorded by Mitie.
- If you are a line manager or are approving requests on behalf of partner or supplier staff, you must ensure that any access rights you approve on staff application forms are valid.
- The Information Governance Team must maintain a list of partners and contractors who are approved to have ECC ID Cards.
- If you are a Commissioner of an external service provider or are managing the relationship with a partner who is authorised to use ECC ID Cards, you must ensure the third party complies with this policy and the Procedure for Managing ID Cards.

## Appendix C – Glossary of terms

This policy may contain some terms you are unfamiliar with, so brief summaries have been provided. You are advised to search online to gain a more in depth understanding of any terms you are unfamiliar with.

| Term | Explanation |
|---|---|
| Anti-malware (also known as anti-virus) | Software products that identify and protect against infections caused by many types of malware, including viruses, worms, Trojan horses, rootkits, spyware, Keyloggers, ransomware and adware. |
| Authentication | The process in which user credentials provided (e.g. ID and password) are compared to those on file in a database of authorised users' information on a local operating system or within an authentication server. Authorisation is granted if credentials match |
| Cloud Computing / Service | Remote computing facilities on demand, accessed via the Internet, and provided by a Cloud Service Provider. NIST provide a clear definition of what is and is not a Cloud service. |
| Configure / Configuration | In the context of this questionnaire, the meaning of configure can be seen as similar to 'setup': When a new device or program is installed, a number of options are sometimes provided to allow it to be configured. The installer choses from these in order to control how the program / device will function, and in a lot of cases this includes setting how secure it will be. Configuration is the way something is configured. More details can be found in the Cyber Essentials scheme. |
| Controls (Security) | Safeguards or countermeasures to avoid, detect, counteract, or minimise security risks to physical property, information, computer systems, or other assets. SANS provide a good write up on these. Search for 'Security Controls' on their site. |
| Data Processing Schedule | Sets out the processing that the Contractor is authorised to undertake. |
| Data Protection Impact Assessment (DPIA) | An assessment by the Data Controller of the impact of the envisaged processing relating to the protection of personal data. |
| Data Protection Officer (DPO) | As formal responsibilities to monitor compliance with the UK General Data Protection Regulation (UK GDPR) |
| Data Subject | An identified or identifiable living individual to whom personal data relates. |
| Data Subject Rights | Means the rights of data subjects as set out in Data Protection Legislation. |
| Direct Marketing | The communication (by whatever means) of advertising or marketing material which is directed to individuals. |
| Encryption (Data) | Translation of data into a secret code. To read an encrypted file, you must have access to a secret key or password, to decrypt it. |

| | |
|---|---|
| Encryption (Full Disk) | All data on the computer's hard disk is converted into a form that cannot be understood by anyone who doesn't have the key to "undo" the conversion. Without the proper authentication key, even if the hard drive is moved into another machine, data remains inaccessible. |
| Firewall (Boundary) | Network device that can restrict inbound and outbound network traffic to services on its network. It helps protect against cyber-attacks by implementing restrictions, known as 'firewall rules', which can allow or block traffic. These are often included in Internet routers. |
| Firewall (Host based) | Software based firewall that works in the same way as a boundary firewall but only protects the device it is installed on. These often come as part of Anti-malware / Internet Security packages and are also included in some operating systems. |
| Hyper Text Transfer Protocol Secure (HTTPS) | This is the secure version of HTTP, the protocol over which data is sent between your browser and the website that you are connected to. The 'S' at the end stands for 'Secure'. In this, all communications between browser and the website are encrypted. Some browsers indicate this by displaying a padlock icon in the address bar. |
| ICT | Stands for 'Information and Communications Technology', which covers any product that will store, retrieve, manipulate, transmit or receive information electronically in a digital form, e.g. PC's , Laptops, Servers, smart phones, and laptops. |
| Information Breach | Means any event that results, or may result, in unauthorised access to ECC data held by the Contractor, and/or actual or potential loss and/or destruction of ECC data, including any personal data breach. |
| Information Handling Schedule | Is a schedule used to ensure that Contractors are complaint with UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. |
| Lockdown build / software | Restrict the functionality / actions a user can perform on a system. e.g. Prevent users from being able to install or de-install applications. |
| Malware | Software which is specifically designed to disrupt, damage, or gain authorised access to a computer system. |
| Multi factor Authentication (MFA) | Provides extra layers of security than just a username and password, requiring two or more independent credentials: what the user knows (password), what the user has (security token for instance, or a code sent to their mobile phone) and what the user is (biometric verification e.g. finger prints for instance). |
| National Cyber Security Centre (NCSC) | The UK's authority on cyber security and part of GCHQ. Their purpose they state is to reduce the cyber security risk to the UK by improving its cyber security and cyber resilience. Provides useful guidance on security: https://www.ncsc.gov.uk/index/guidance. This includes videos on Information Security for Small Businesses. |

| | |
|---|---|
| Network (Internal) | A company's private network on which their internal IT systems sit. This may be connected to the Internet via a firewall / router. |
| Network (Perimeter) | The boundary between the private and locally managed-and-owned side of a network and the public and usually provider-managed side of a network (internet). |
| Network (Trusted) | A network that is under the control of the organisation (network manager / administrator) |
| Network (Untrusted) | A network that is external to the networks belonging to an organisation, and which is out of the organisation's ability to control or manage. The Internet is an example of an untrusted network. |
| Outcomes | The way something turns out, or you want it to turn out. Something that occurs as a result of actions taken. In the context of this policy, one of the required outcomes is protecting the solution / service from malware, as a result of implementing appropriate security controls (antimalware software and controls). |
| Penetration test | Authorised simulated attack on a computer system that attempts to exploit vulnerabilities to determine whether unauthorised access or other malicious activity is possible. Manual penetration tests layer human expertise on top of professional testing software and tools. |
| Privileged access | Access permissions greater than those of a 'standard' user account. This may allow the account to access additional data or make changes to settings and install software. Some privileged accounts have dedicated names such as Administrator. |
| Remote wipe facility | A facility that allows an administrator to send a signal to a lost or stolen device to locate it, and if necessary, securely delete its data. |
| Removable media | Any type of storage device that can be removed from a computer while the system is running. Examples include CDs, DVDs, Blu-Ray disks, Memory sticks and other USB based storage media. |
| Retention Schedule | Is a policy that defines how long data items must be kept and provides disposal guidelines for how data items should be discarded/destroyed. |
| Secure Baseline build / Standard build / Standard configuration / Gold build | A minimum specified security configuration created for ICT systems, covering clients, mobile devices, servers, operating systems, network devices (e.g. firewalls and routers) and applications. Functionality, services, and applications that are not required are removed or disabled. Builds are subject to configuration control, and any deviation or changes made, documented and formally approved. |
| Strong / Complex passwords | These generally consist of 9 alphanumeric characters or more, which are a mixture of upper and lower case, the use of 'special characters' (non-alphanumeric characters such as £$%^&#) and do not contain real words. The objective of this is to make the passwords more difficult to guess or work out. Please see the NCSC guidance. |

| | |
|---|---|
| Sub-Processor Arrangement | Any third party appointed to process data on behalf of ECC via a main contractor processor. |
| Two factor authentication (2FA) | A form "multi factor authentication" requiring an additional piece of authentication information to be entered into a system, in addition to a user's ID and password, before granting access. This must be something that *only* that user has, such as a physical token or code texted to mobile phone. For more details, please see the 'Multifactor Authentication' definition. |
| User account (Standard) | An account that is restricted but allows users to perform general day to day activities. It cannot be used however to perform such actions as install or modify software and change system settings. |
| User account (Privileged) | An account that has permissions additional to that of a 'standard' user account. This may allow the account to access additional data or make changes to settings and install software. Some privileged accounts have dedicated names such as Administrator. |
| Virtual Private Network (VPN) | Technology that creates a safe and encrypted connection over a less secure network, such as the internet. Data travels through secure tunnels and to gain access, VPN users must use authentication methods such as passwords, tokens, and other unique identification methods. VPN was developed as a way to allow remote users / branch offices, secure access to corporate applications/ resources.<br>NCSC End User Device VPN guidance. |
| Vulnerability scan | A scan of computers, networks, and communications equipment that identifies classifies and reports on vulnerabilities (weaknesses) found, and appropriate counter measures available. A number of vulnerability scanning tools are available that perform this function. |
| Web Content filtering | The use of a program or service that screens and excludes from access Web pages that are deemed to be unsafe or inappropriate. The filter checks the origin or content of a Web page against a set of rules provided. This facility can be found in complete online services, dedicated software, and also some anti-malware and Internet Security products |

A glossary can also be found on the NCSC site together with an Infographic