bbfc

Age-verification Certificate Standard

April 2019

Contents

1. Introduction to the Standard

The Digital Economy Act 2017 (henceforth ‘DEA 2017’) requires that commercial online pornographic services put in place controls that ensure that it is not normally possible for children to access pornographic content online. As the Age-verification Regulator, the British Board of Film Classification (BBFC) encourages age-verification providers to develop age-verification solutions that are effective and follow an approach of data protection by design and by default. To that end, this document is the age-verification certificate standard (the Standard), and this is the foundation of the non-statutory, voluntary age-verification certification scheme (the Scheme).

The Scheme has been created to offer age-verification providers an opportunity to demonstrate to consumers that their solutions meet the BBFC’s high standards in relation to age-verification, particularly as regards data protection and information security. In particular, ensuring effective measures are in place for pseudonymisation, data minimisation and secure storage. Only age-verification providers that meet the requirements of the Standard in full, as assessed by a suitably qualified independent third party, will receive certification. The certification process is outlined within the associated Programme Guide and this standard should be read in conjunction with the associated Programme Guide.

The BBFC will govern this non-statutory certification scheme for those age-verification providers who volunteer to submit their solutions for assessment. The BBFC will also provide the certification. This is in addition to, and separate from, the BBFC’s assessment of commercial online pornographic services' compliance with the requirement under section 14(1) of the Digital Economy Act 2017.

This Scheme, which is a voluntary, non-statutory certification of age-verification solutions, is not a certification scheme as defined within the European Union’s General Data Protection Regulation (GDPR) or the United Kingdom’s Data Protection Act 2018 (DPA 2018). Certification under this Scheme does not represent a statement of compliance with either GDPR or the DPA 2018. To that end the Information Commissioner’s Office (ICO) are not required to take the Scheme into account when considering regulatory action against age-verification providers.

2. Purpose

The purpose of the Standard is to outline the control requirements that age-verification providers must meet in order to become certified under the voluntary certification scheme. Only age-verification providers that meet the requirements of the Standard in full, as assessed by a suitably qualified independent third party, will receive certification. The certification process is outlined within the associated Programme Guide, which the Standard should be read in conjunction with. Further guidance on specific industry guidance and standards referred to throughout the Standard can be found in the Programme Guide.

3. Scope of the Standard

Age-verification providers conducting age-verification checks on individuals seeking to view online pornographic content in the United Kingdom. Further guidance around the scope of certification can be found in the Programme Guide.

4. Objective

By meeting the requirements of the Standard age-verification providers shall be able to demonstrate that a framework of data protection and information security controls have been implemented, their solution has been developed by following the principles of data protection by design and by default and the privacy of users shall be maintained

5. Principles

This Standard is based on the following principles:

- **Flexibility**: the Standard is flexible enough to respond to developments in age-verification technology, processes and legislation
- **Data Protection**: the Standard follows the principles outlined in the DPA 2018 and the GDPR. In particular, age-verification providers shall maintain the privacy of users and only process personal data:
    - in a lawful, fair and transparent manner
    - for purposes that are not incompatible with the original purpose for collection
    - if it is required to fulfil the purpose for processing
    - if it is accurate and up-to-date
    - for a specific period of time before it is destroyed, deleted or anonymised
- **Security**: the Standard will ensure the appropriate technical and organisational measures shall be in place to ensure the confidentiality, integrity and availability of age-verification solutions
- **Selection**: the Standard will not force age-verification providers, implicitly or explicitly, into selecting particular age-verification methods or data sources.

6. Definitions

Age-verification Provider – A company which supplies an age-verification method or solution to an online pornographic service.

Age-verification Gateway – A company which provides users with access to third party age-verification solutions or methods.

Age-verification Solution – The mechanism used by an age-verification provider to validate a user’s age based on an age-verification method.

Age-verification Method – The means by which age-verification (or age checking) is achieved (e.g. use of an ID document or credit card).

User – An individual or person visiting a website that requires age-verification.

Any data protection related terms used throughout the Scheme are as the definitions cited in the GDPR and DPA 2018.

7. Penetration Testing Methodology

As outlined within the Programme Guide, age-verification providers must undertake a penetration test in order to become certified. Penetration testing is a method of testing a computer system, web application or network to find security vulnerabilities that an attacker could exploit. Penetration tests shall be completed based on industry recognised methodologies and shall require testing of both the network and applications layers.

A list of industry recognised methodologies, such as the OWASP Testing Guide, can be found in the Programme Guide. The scope of penetration tests should comprise all external IP addresses and internal network segments associated with the age-verification solution that could allow a malicious entity to exploit a security vulnerability (that is either a logical or a physical perimeter) and gain unauthorised access to the age-verification solution or compromise the security, privacy or functionality of the age-verification solution or its associated infrastructure. All penetration tests must comprise of:

- Internal and external network penetration tests, which comprise of a full network-layer attack to identify and subsequently exploit any weaknesses or vulnerabilities that could be used by a malicious entity to gain access to the age-verification providers' infrastructure. Network infrastructure equipment and servers should also be exposed to a configuration hardening review conducted on the host (a sampling approach is acceptable where common base builds are utilised)
- Application tests, which shall be completed using credentials supplied by the age-verification provider to ensure that the controls implemented suitably restrict users of the solution or solution administrators from inadvertently or maliciously gaining elevated privileges or functionality within the application. These tests should be white-box in nature with full documentation of any web service requests for example supplied to the testing organisation
- Segmentation testing, which shall provide assurance that any network segments intended to be isolated from the wider corporate or other networks, including any management infrastructure, are truly isolated. Network segmentation can be used to minimise the scope of the assessment providing that independent testing and assurance of the segmentation is obtained at least annually or following any significant changes. This can be performed by network diagram review, firewall access control list review and also as part of the penetration testing scope.

8. Domains and Control Requirements

The domain and control requirements listed below are to be implemented and maintained by an age-verification provider in order to qualify for, and maintain, an age-verification certificate issued by the BBFC.

Further guidance on the certification process can be found in the Programme Guide, including examples of specific industry guidance and standards which are referred to throughout the controls.

8.1 Governance

8.1.1 Policy Framework

A policy framework shall be created which provides direction on how the information security and data protection requirements of this Standard are implemented within the organisation. A process shall be in place to ensure policies are reviewed annually or after any significant change.

8.1.2 Senior Management Commitment

Senior management shall approve the policy framework and complete annual reviews of its suitability and efficacy.

8.1.3 Roles and Responsibilities

Roles and responsibilities associated with information security, data protection and operational activities shall be clearly defined and documented.

8.1.4 Audits

Audits of policy, legal and regulatory compliance shall be completed at least annually.

8.1.5 Risk Management

A risk management framework shall be implemented for the identification, assessment, ownership and management of information security and data protection risks.

8.1.6 Physical Asset Management

All physical assets shall be documented and maintained in registers with details of the asset, asset owner, asset classification and impact of loss, compromise or unintended disclosure.

8.1.7 Digital Asset Management

All digital assets such as software, information assets and backups shall be documented and maintained in registers with details of the asset owner, classification, version numbers if applicable and impact of loss, compromise or unintended disclosure.

8.1.8 Age-verification Policy

An age-verification policy shall be implemented that details the organisation's approach to ensuring ongoing quality and accurate age-verification checks.

8.1.9 Communicating Service Changes

Users shall be notified of changes to how the age-verification provider processes personal data for the purpose of age-verification.

8.1.10 Preventing Use by Non-Human Operators

The age-verification service shall include measures which are effective at preventing use by non-human operators including challenge–response tests and algorithms.

8.1.11 Customer Service

Policies and processes shall be implemented and maintained for handling customer queries and complaints, including providing a specific point of contact.

8.1.12 Legal, Regulatory and Contractual Requirements

The organisation's approach to meet all relevant legal, regulatory and contractual requirements shall be centrally documented and kept up to date.

8.1.13 BBFC Notification and Reporting

Certified age-verification providers shall follow the notification and reporting requirements outlined in the Programme Guide. For example, following a material change to the certified age-verification solution.

8.2 Secure Workforce

8.2.1 Background Checks

All potential employees and contractors shall be subject to background checks in accordance with the level of risk based on their role / responsibility in line with all relevant laws, ethics and regulations.

8.2.2 Training and Awareness

All employees and contractors shall complete quality information security and data protection training upon employment and on an annual basis. This shall include an acknowledgement of receipt and understanding of key policies.

8.2.3 Specialised Training

Targeted training shall be provided to employees and contractors with elevated information security responsibilities, with privileged access and those involved in key data protection processes such as data protection impact assessments, responding to data subject rights and incident management.

8.2.4 Workforce Responsibilities

All employees and contractors shall formally acknowledge their individual information security and data protection responsibilities. All employees and contractors shall be provided with the support required to fulfil their responsibilities.

8.2.5 Confidentiality Agreements

Confidentiality agreements shall be in place with all employees, contractors or third parties that access or come into contact with commercially or personally sensitive information.

8.2.6 Acceptable Usage Policies

The organisation shall determine and document acceptable and unacceptable uses of technology, access and other assets made available to employees during the course of their employment.

8.3 Access Control

8.3.1 Access Control Policy

An Access Control Policy shall be established, documented and reviewed based on what is reasonable for the role and information security requirements in line with the need-to-know principle.

8.3.2 Provisioning Access

Access to systems and information shall be provided on a principle of least privilege basis and following a formalised process.

8.3.3 Terminating Access

Access to systems and information shall be revoked immediately when no longer required by employees, contractors or external parties.

8.3.4 Privileged / Administrative Account Management

Privileged / administrative accounts shall be subject to a documented approval process and only used when required for administrative activities. They shall not be used for email or web browsing. All privileged / administrative accounts shall be reviewed on a monthly basis and multi-factor authentication shall be used where technically possible. Passwords shall be set to at least 15 characters and comprise of upper and lower case letters, numbers and special characters. Controls shall be in place to ensure commonly known or previously breached passwords are not used.

8.3.5 Reviews of Access

Access to systems, buildings and information shall be reviewed on at least a biannual basis and removed when no longer required.

8.3.6 Remote Access

All remote access shall be explicitly approved, individually assigned, use secure connection mechanism and monitored for appropriate use. Access to network resources from untrusted networks must use multi-factor authentication. Third party remote access shall only be provided when there is a documented business justification.

8.3.7 Mobile Technology Security

All technology that is inherently mobile including but not limited to, removable media, laptops and mobile phones shall be protected. Protection shall include, but not limited to, industry standard encryption and the ability to remotely wipe data.

8.3.8 Identification and Authentication

All access to systems, networks, buildings and information shall use individually assigned accounts, appropriate authentication mechanisms based on the classification of the asset and access shall only be provided to authorised information and functionality previously approved. If passwords are used they shall be set to at least eight characters and comprise of upper and lower case letters, numbers and special characters. Controls shall be in place to ensure commonly known or previously breached passwords are not used.

8.3.9 Service Accounts

All service accounts used for system-to-system authentication shall be assigned the minimum access required to perform its role, shall be individually owned. and passwords shall be set to at least 15 characters and comprise of upper and lower case letters, numbers and special characters. Controls shall be in place to ensure commonly known or previously breached passwords are not used.

8.3.10 Default Credentials

All default credentials for systems, applications, mobile technology, infrastructure and network components, including restricting management interfaces to private networks, shall be changed as soon as possible, and at least prior to deployment.

8.3.11 Software Installation

Software shall only be installed from previously approved software suppliers or after due diligence checks and testing have been completed in accordance with defined, documented processes and procedures.

8.4 Operational Security

8.4.1 Installation Standards

All digital and physical assets shall be configured in line with industry standards or shall provide the minimum functionality required to enable the device to fulfil its purpose.

8.4.2 Change Management

Changes to IT infrastructure, business processes, delivery or provision of goods or services from third parties and other changes shall be controlled, assessed, approved and implemented with information security and data protection evaluated at all stages.

8.4.3 Anti-Malware

Anti-malware software shall be installed on all devices where technically possible. This must be updated regularly (in line with updates from software providers) to detect and prevent the infection of hosts.

8.4.4 Information Classification, Labelling, Handling and Destruction

Information shall be classified in accordance with its sensitivity and appropriately labelled. In addition, the organisation shall determine the appropriate handling and destruction practices required based on the classification scheme. Employees and contractors shall be trained on the understanding, implementation and requirements of the data classification scheme.

8.4.5 Device Re-use and Destruction Lifecycle

All devices being repurposed, requiring destruction or being sent for repair shall be securely stored, wiped and all software licences removed. Destruction practices should be in line with the classification of the asset and in accordance with industry standards.

8.4.6 Messaging Security

Email and end-user messaging technology used as part of an age-verification method shall be protected using industry standard encryption. All email and end-user messaging technology shall be protected using spam and malware filtering and any additional controls as required.

8.4.7 Logging of Physical and Digital Assets

All physical and digital assets shall produce logs from all accounts, including privileged and administrative accounts, which includes activity, suspicious or anomalous events and configuration changes. Logs shall be protected from access, alteration or disclosure, promptly backed up and retained for at least 12 months.

8.4.8 Logging of Age-verification Checks

Logs for age-verification checks shall not be generated and retained unless required for fraud prevention and detection. Logs shall not contain information used to verify an individual’s age or information about the website the user has visited. Logs shall be protected from access, alteration or disclosure. Logs for age-verification checks shall only be retained for the length of time required to prevent or detect fraudulent activity from taking place.

8.4.9 Monitoring Critical Assets

All logs produced by critical physical and digital assets shall be reviewed daily using automated solutions or manually in accordance with a documented policy and procedure.

8.4.10 Monitoring Other Assets

All logs produced by non-critical physical and digital assets shall be regularly reviewed using automated solutions or manually in accordance with a documented policy and procedure.

8.4.11 Time Sources

The time sources / clocks for all relevant physical and digital assets shall be synchronised to a single time source.

8.4.12 Cryptography Policy

A policy shall be implemented to ensure cryptographic controls are used to protect information used to verify an individual’s age at rest and in transit.

8.4.13 Cryptographic Key Lifecycle

A policy and associated procedures shall be created to identify the responsible parties for cryptographic key generation, storage, revocation, issuance and security.

8.4.14 Fraud Prevention and Detection

Real-time intelligent monitoring and fraud prevention and detection systems shall be used for age-verification checks completed by the age-verification provider.

8.4.15 File Integrity Monitoring

Core files, configurations and rule sets of critical assets, or assets providing security functions shall be monitored and an automated alert or notification issued to the relevant party upon identification of alterations.

8.4.16 Network Topology

Network diagrams shall be implemented and maintained to accurately represent the network topology. These shall be reviewed at least annually or after any significant change.

8.4.17 Network Controls

Network controls shall be implemented to provide protection against common cyber-attacks, to protect data in transit and to segregate physical or digital assets that do not need direct interaction.

8.5 Data Protection

8.5.1 Data Controller / Processor Relationships

Age-verification providers shall define and document whether they are acting as a data controller or data processor for the purposes of age-verification checks.

8.5.2 Data Protection Impact Assessment

A data protection impact assessment of the age-verification solution shall be completed to identify, assess and reduce the security and privacy risks of the service. If the age-verification provider highlights any risk that cannot be mitigated they shall consult the appropriate supervisory authority before starting the processing, in line with data protection legislation. Personal data flow diagrams of each age-verification method shall also be documented.

8.5.3 Data Protection by Design and by Default

Data protection by design shall be implemented within all relevant business processes. The age-verification service shall be designed to ensure user's personal data is protected by default.

8.5.4 Fair and Transparent Processing

In line with data protection legislation, users shall be informed about why, when, where and how their personal data is being processed, and by which organisations. Where an organisation processing personal data is based outside the European Economic Area (EEA), an EEA-based representative shall be appointed and notified to the user.

8.5.5 Lawful Processing

A lawful basis for the processing of any personal data, in line with the requirements of data protection legislation, shall be identified and documented for the purposes of age-verification and fraud prevention and detection.

8.5.6 Data Minimisation

Only the minimum amount of personal data required to verify a user's age shall be collected. A user's identity shall not be verified as part of the process. Information about the requesting website that the user has visited shall not be collected against the user's activity.

8.5.7 Pseudonymisation

Only industry standard pseudonymisation techniques and appropriate technical and organisational controls shall be implemented to ensure any information that can be used to re-identify an individual is tightly controlled. There shall be a clear separation between personal data used to verify an individual is 18 or over and any pseudonymous credentials that are generated.

8.5.8 Sharing Results

Age-verification providers shall only share the result of an age-verification check (pass or fail) with the requesting website.

8.5.9 Physical Location

Personal data relating to the physical location of a user shall not be collected as part of the age-verification process unless required for fraud prevention and detection. Personal data relating to the physical location of a user shall only be retained for as long as required for fraud prevention and detection.

8.5.10 Retention

Personal data used for age-verification checks and fraud prevention and detection shall not be kept for longer than is necessary for this purpose.

8.5.11 Failed Verification

Personal data about visitors who fail age-verification checks shall not be retained but instead securely deleted and / or destroyed unless required for fraud prevention and detection.

8.5.12 Purpose Limitation

Personal data used for fraud prevention and detection and to verify a user's age for access to commercial online pornographic material shall not be used for any other purposes, such as marketing or the creation of digital wallets. Age-verification providers shall not market other services to these users during or after the age-verification process. If a user has already created an account with an age-verification provider for the provision of a different service, such as age-verification for websites related to gambling, age-verification providers are able to continue processing that user's personal data for those purposes.

8.5.13 Guest Verification

A user shall be given the option to verify their age without being required to set up an account with the age-verification provider.

8.5.14 Data Accuracy

The age-verification provider shall take all steps necessary to ensure the personal data processed to verify a user's age is accurate and up to date.

8.5.15 International transfers

Age-verification providers shall only transfer personal data outside the European Economic Area to a country whose data protection laws have been approved by the European Commission. If approval is not in place for a particular country, age-verification providers must implement additional safeguards as allowed for in data protection legislation.

8.5.16 Data Subject Rights

Procedures shall be in place to respond to requests from users wishing to exercise the following rights under data protection legislation:

- Right of access
- Right to erasure
- Right to rectification
- Right to object
- Right to restriction
- Data portability
- Automated decision making.

8.5.17 Record of Processing Activities

A record of all processing activities that relate to the age-verification solution shall be documented and maintained to meet the requirements outlined within Article 30 of the GDPR

8.6 Secure Development

8.6.1 Security in the Software Development Lifecycle

A policy shall be implemented to provide clear guidelines on how information security and data protection are incorporated into the software development lifecycle.

8.6.2 Coding Updates

Updates to software coding shall be tightly controlled and must be reviewed, approved and tested prior to release. All coding updates are to be approved by a change board or similar to ensure that the change does not having a negative or undesired impact.

8.6.3 Secure Coding

Secure programming guides from industry recognised sources shall be utilised for each coding language in use and applied to any information system implementation efforts.

8.6.4 Separation of Environments

Production environments shall be segregated from test or development environments.

8.6.5 Code Reviews

Code changes shall be reviewed by individuals who are appropriately trained and experienced. Reviews shall not be conducted by the originating code author.

8.6.6 Code Testing

Tests shall be completed to ensure coding updates do not impact the functionality, security or auditing elements of the application.

8.6.7 Test Data

Test data shall never contain personal data from production environments.

8.6.8 Secure Age-Verification Checks

Age-verification providers shall protect requests, responses and / or transactions that pass over the internet from interception, manipulation, alteration, re-use and unauthorised disclosure.

8.6.9 Source Code Protection

Source code shall be protected from unauthorised disclosure, deletion, alteration or access.

8.6.10 Outsourced Development

Procedures shall be implemented to ensure any outsourced development meets the requirements listed within this domain.

8.7 Third Party / Data Processor Management

8.7.1 Third Party Management Policy

A policy shall be implemented to outline how information security and data protection risks are identified and managed throughout the third party lifecycle. A register of all third parties (including all data processors) shall be maintained along with a business owner for each relationship.

8.7.2 Third Party Due Diligence

Due diligence checks shall be conducted of all third parties prior to the engagement of the service and on an ongoing basis. The level of due diligence shall be based on a risk assessment of the third party; in particular for third parties identified as data processors or involved in the age-verification process. Only third parties, including data processors and sub processors, that are able to evidence that they meet the requirements of applicable data protection legislation shall be used.

8.7.3 Contracts with Third Parties

All third parties, including data processors and sub processors, shall operate under a written contract which shall comply with each party's legal and regulatory requirements.

8.7.4 Third Party Responsibilities

Age-verification providers and third parties who can impact, or who are responsible for maintaining, security and privacy controls shall clearly document each party’s responsibility in implementing and maintaining the relevant controls of this Standard.

8.7.5 Third Party Changes

Changes to the services provided, including the use of new data processors or sub-processors, shall result in the re-completion of the due diligence process to ensure any additional risks are identified, documented and mitigated.

8.7.6 Cessation of Third Party Relationships

Measures shall be put in place to ensure that when a relationship with a third party is ending all access or information provided to provision services is securely destroyed, returned or revoked.

8.7.7 Third Party Information Sharing

Only the minimum amount of personal data required to verify a user's age shall be shared with third parties involved in the age-verification process. Information about the original requesting online pornographic service shall never be shared with third parties involved in the processing of verifying a user's age.

8.8 Physical Security

8.8.1 Physical Security Policy

A policy shall be documented and implemented to define areas of different sensitivity and the controls that are required to be implemented based on the sensitivity of the area or location.

8.8.2 Visitor Process

A visitor process shall be implemented to reduce the likelihood of unauthorised physical access and to manage visitors during the time period that they are on site.

8.8.3 Clear Desk/Screen Policy

A clear desk/screen policy shall be implemented and maintained to avoid the accidental or malicious use of systems, disclosure of information or loss of media.

8.8.4 Remote/Homeworking

Guidelines shall be implemented to ensure employees and contractors working remotely are aware of their information security and data protection responsibilities and how to manage the inherent risks of working outside an age-verification provider's premises.

8.9 Vulnerability Management

8.9.1 Solution Testing

Penetration testing of age-verification solutions directly accessible by the public shall be tested by a suitably qualified individual at least annually or after a significant change.

8.9.2 Internal Penetration Testing

Penetration testing of an age-verification provider's internal network shall be conducted by a suitably qualified individual at least annually or after a significant change.

8.9.3 External Penetration Testing

Penetration testing of an age-verification provider's public-facing infrastructure shall be conducted by a suitably qualified individual at least annually or after a significant change.

8.9.4 Segmentation Testing

If network segmentation is used, penetration testing of the segmentation shall be completed by a suitably qualified individual at least annually or after a significant change.

8.9.5 Technical Vulnerability Notifications

Vulnerability notifications shall be received from industry recognised sources for all technology, software, applications and tools in use and shall be individually or centrally assessed in a timely manner in order to meet the vulnerability treatment timelines outlined within this domain.

8.9.6 Technical Vulnerability Assessments

Vulnerability notifications received from industry recognised sources, as a result of penetration tests or vulnerability assessment shall be assessed and rated in accordance with the risk management framework, using industry sources such as the Common Vulnerability Scoring System, to identify the impact to the age-verification provider's security posture.

8.9.7 Technical Vulnerability Treatment

Remediation activity shall be undertaken to mitigate any vulnerabilities as soon as is practically possible, and in any case vulnerabilities with a risk rating of critical must be remediated within 14 calendar days and risks identified as high must be remediated within two months. Penetration tests and vulnerability assessments shall be repeated until no critical or high risks are identified.

8.9.8 Patching

All vendor-supplied patches shall be installed as soon as is practically possible and in any case critical security patches shall be applied to system components within 14 calendar days of their release and non-critical vendor-supplied security patches shall be applied within two months.

8.9.9 Supported Technology

All hardware, systems and applications shall be within vendor support or utilise additional controls to protect the confidentiality, integrity and availability of the asset.

8.9.10 Network Vulnerability Assessments

Vulnerability assessments shall be completed on all external and internal infrastructure quarterly or after a significant change.

8.10 Incident Management

8.10.1 Incident Management Documentation

An incident management policy and plan shall be implemented and maintained which document actions, roles and responsibilities in the event of an information security or data protection incident.

8.10.2 Incident and Vulnerability Reporting

A defined process shall be established to ensure all employees, contractors and third parties are aware how to report incidents and weaknesses and how to triage or escalate incidents if necessary.

8.10.3 Incident Log

A log of all actual or suspected incidents shall be maintained which includes records of 'near misses' and include details of the incident and steps taken to address including whether the incident was reported to any regulatory body. This log shall be periodically reviewed to identify patterns or trends.

8.10.4 Evidence Handling

Evidence shall be securely collected and stored when investigating events, weaknesses or incidents.

8.10.5 Incident Management Communications

External stakeholders shall be provided notifications during, and following an incident in line with legal, regulatory and contractual requirements.

8.10.6 Learning and Evolving

Post-incident reviews shall be completed to identify any opportunities to reduce the likelihood of similar incidents occurring.

8.10.7 Incident Management Plan Testing

The plan shall be tested at least annually or after a significant change to ensure it is still adequate, effective and known by all relevant parties.

8.11 Resilience

8.11.1 Business Continuity/Disaster Recovery

Business recovery and continuity plans shall be in place to ensure systems/services can be restored to normal operations in accordance with documented recovery time and recovery point objectives.

8.11.2 Backup

Backups of data, system images and configuration files shall be captured in accordance with a documented backup schedule, securely stored and shall be tested regularly.

8.11.3 Resilience Testing

Business recovery and continuity plans shall be tested annually or following significant changes to ensure they are still adequate, effective and known by all relevant parties.

Lessons learned from the tests shall be documented and incorporated into updated plans.

End of document.