ELA Training Services

Information Security Policy Technical Controls

1st March 2023
V1.0

Contents

Contents 2
1. Document History 3
2. Document Objectives 3
3. Document Structure 3
4. Document Control 3
5. Security Policy Management 4
5.1 Management of Information Security Policies 4
5.2 Compliance Review Process 4
6. Physical and Environmental Security – Server Rooms/Comms Cabinets 4
6.1 Physical Access to Server Room 4
6.2 Conduct in Server Room 5
6.3 Environmental Controls in Server Room 5
6.4 Public access, delivery, and Loading Areas 6
6.5 Equipment siting and protection 6
7. Communications and IT Operations Management 6
7.1 Documented Security Operating Procedures 6
7.2 Change Management 6
7.3 Segregation of Duties 7
7.4 Separation of Development, Test and Operational Facilities 7
7.5 Third Party Service Delivery Management 7
7.6 Protection Against malicious and Mobile Code 7
7.7 Availability Monitoring and Management 9
7.8 Backup and Data Restoration 9
7.9 Secure Disposal 10
7.10 Management and Configuration of Servers 10
7.11 Management and Configuration of Routers, Switches and Firewalls 11
7.12 Wireless Computing 11
7.13 Exchange of information 11
7.14 Audit Logging 11
7.15 Clock Synchronization (Network) 12
7.16 Fault Logging 12
8. Access Control 12
8.1 Overall Approach to Access Controls 12
8.2 Log-in and Password Controls 13
9. Information Systems Acquisition, Development and Maintenance 16
9.1 Security requirements of information systems 16
9.2 Security of system files 16
9.3 Technical Vulnerability Management 17
9.4 Testing of New Systems 17

Document History

Issue	Issue Date	Author	Revision Notes
1	20th February 2023	MJ	Draft v 0.01 – First Draft
2	21st February 2023	MJ	Draft v0.01 Amends
3	22nd February 2023	MJ	Draft v0.01 Amends
4	1st March 2023	MJ	Move from Draft to release V 1.0

Document Objectives

In relation to Personal Identifiable Information (PII) this document sets out the technical controls that together with 'Information Security Management – Organisational Controls' ensure effective information security is in place throughout ELA.

This policy encompasses information that is stored in both electronic and paper-based formats or processing systems.

Document Structure

The structure of this document is based broadly on the global information security standard ISO 27001.
There are a total of 9 main sections. Each section addresses a specific set of controls designed to address particular threats, risks, and vulnerabilities. However, with the exception of the Information Asset Owner, Policy makers and Senior management (who must read the document in its entirety and sign off as part of the Corporate governance) the document is designed to be read as a reference document.

Each section contains one or more policies. A policy is an overall statement of intent and direction.

Most policies in turn have procedures associated with them. These are specific controls and requirements aimed at ensuring the policy is implemented effectively.

Some policies also have standards associated with them. These are essentially specifications (e.g., prescribed settings for a security device) as opposed to the "how to" nature of procedures.

Document Control

ELA's information security policies and procedures are living documents. Reviews will be conducted, at a minimum annually, by the ELA Risk Assurance team (and if necessary, the Data Compliance Manager) to ensure that the policies and procedures are continuing to achieve their purpose as a practical operational framework for ensuring a suitable level of security for ELA, its clients, learners, suppliers, and other 3rd Parties.

The ELA Risk Assurance Team (refer to the Information Security Management – Organisational Controls Policy) is responsible for ensuring that the information security policies and procedures continually align with ELA's operational requirements and reflect ELA's overall requirements for effective risk management.

All revisions to the information security policies and procedures must be agreed by the ELA Risk Assurance team.

Security Policy Management

5.1 Management of Information Security Policies

ELA.'s management team is committed to ensuring that the company's information security policies and procedures properly reflect ELA.'s business requirements and are in line with all relevant laws and regulations.

ELA.'s management will take all necessary steps to ensure compliance with the company's information security policies and procedures at all times. A Security Threat and Countermeasures Register will be kept comprising a list of all known perceived threats and countermeasures and a target date for the resolution of the non-compliance

5.2 Compliance Review Process

The ELA Risk Assurance Team is responsible for monitoring compliance with the information security policies and procedures.

It is recognised that from time to time operational or commercial imperatives may require a level of departure from the policies and procedures, but all actions must remain within accepted risk tolerance and be legally compliant.

Physical and Environmental Security – Server Rooms/Comms Cabinets

6.1 Physical Access to Server Room

This policy (and its associated procedures) shall apply to ELA Server Room(s)

To ensure that there is no unauthorised access to the Server Room, access will be controlled at all times.

6.1.1 Server Room Access Procedure

Access to 3rd party IT Provider / ELA Server Room shall be restricted by use of an issued swipe card, key fob or PIN entry lock that is only issued to employees/approved 3rd party contractors who need access to the Server Room as a part of their normal duties.

Access to the data centre will be logged and records kept for regular audit purposes.

Access codes may only be issued by the Head of MIS, Compliance & Admin, Head of IT Operations (or authorised deputy), or a member of Executive Committee and under no circumstances may employees pass their codes on to, or share their swipe cards with, any other person.

6.1.2 Monitoring Physical Access

Server Room access logs will be accessible for audit and management purposes to the Head of MIS, Compliance & Admin and the Head of Human Resources.

The Head of MIS, Compliance & Admin will monitor the access log on a regular basis and shall inspect it at least quarterly. If any unusual patterns or other suspicious information is found within the log, then the Head of MIS, Compliance & Admin and the HR Manager shall meet to determine a suitable investigative process.

6.1.3 Procedure for Revoking Physical Access

The Server Room access code will be changed in any of the following circumstances:

- If a relevant employee is suspended from their duties for whatever reason
- If a relevant employee is about to be absent for a period longer than three working weeks for whatever reason (holiday, assignment elsewhere, illness)
- If either the Head of MIS, Compliance & Admin or member of the Executive Team have reasonable grounds for believing that it is in the interests of ELA to temporarily suspend an employee's right of access to the Server Room.
- When a relevant employee leaves or changes job, the new code will be communicated to all employees who have authorised access.

6.1.4 Server Room Visitors Procedure

On occasion, it may be necessary for visitors to access an ELA Server Room temporarily (e.g. facilities/maintenance teams, technicians from 3rd Parties who supply hardware or software to ELA, security auditors, etc.).

No visitor shall be provided with an access code. Instead, the visitor shall be escorted into the Server Room by an authorised employee who shall remain with the visitor at all times whilst the visitor is in the Server Room and will be responsible for ensuring the appropriate behaviour of the visitor whilst in the Server Room.

6.2 Conduct in Server Room

Staff and visitors will at all times adhere to the conduct requirements when in the Server Room.

Anyone seeing behaviour that is in breach of this policy should report the matter immediately to the
Head of MIS, Compliance & Admin who shall then take appropriate action.

6.2.1 Conduct within the Server Room

The server room is critical to business operations. Accordingly, it needs to be a controlled environment
to ensure that ELA facility maintains uninterrupted computing services.

In order to adequately protect the server room and the equipment contained therein, the following activities are strictly prohibited within the server room at any time:

- Smoking.
- Drinking.
- Eating.
- Littering.
- Other inappropriate behaviour.

No employee shall tamper with or do anything that could interfere with the proper operation of any of the server room environmental controls.

6.3 Environmental Controls in Server Room

All ELA server rooms will comply with the environmental controls set out in ELA Server Room Environmental Standard.

6.3.1 Protecting the Server Room Environment

Suitable environmental controls shall be implemented and maintained at all times in ELA server room to ensure (as far as reasonably possible) uninterrupted computing services for ELA and its customers.

6.3.2 ELA Server Room Environmental Standard

The server room shall contain the following environmental control features:

- Air conditioning
- Secure power supply system.
- Emergency power off switches.
- Fire extinguisher.

All IT Assets contained within the server room and in distribution switch cabinets must be protected from power failures and other electrical anomalies. This will be achieved through the following measures:

- All power supplies used shall conform with the equipment manufacturer's recommendations.
  The IT Department shall maintain a supply of approved power connectivity equipment (plugs, leads etc.) and shall ensure that items from this supply are used in respect of any IT Asset.
- Multiple power feeds are installed where possible to avoid a single point of failure in the power supply.
- An uninterruptible power supply ("UPS") will be installed to support orderly close-down or continuous running of all equipment in the server room.
- The UPS shall be tested at three monthly intervals in accordance with the manufacturer's instructions.
- Emergency power switches shall be located near emergency exits in server rooms to facilitate rapid power down in case of emergency.
- Emergency lighting will be available in case of main power failure. Lightning protection shall be applied to all buildings and lightening protection filters shall be fitted to all external communications lines.

All perimeter devices (such as firewalls and routers) must be provided with special protection. This will be achieved through the following measures:

- The racks containing perimeter devices shall be in a cabinet within the server room, labelled accordingly.
- Any work necessary on any perimeter device may only be undertaken by (or, if undertaken by an external contractor, under the personal supervision of) one of the key holders to the perimeter device cabinet.

6.4 Public access, delivery, and Loading Areas

Access points such as delivery and loading areas and other points where unauthorized persons may enter the premises shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.

6.5 Equipment siting and protection

Equipment shall be sited or protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.

7.1 Documented Security Operating Procedures

All IT Systems will have associated version-controlled Security Operating procedures that will be made available to users. Documentation is protected against unauthorised access via electronic controls imposed by Active Directory.

SSL and secure certificates encrypt email and web-based content as required during transmission.

7.2 Change Management

Any change to IT infrastructure has the potential to cause operational problems and can also give rise to increased security risks. Changes to the ELA network (hardware or software) and data structures therefore need to be carried out in a controlled manner, with proper planning and consultation with impacted users.

All changes to the IT infrastructure shall be made using ELA Change Management Procedure. These procedures cover all changes to the ELA IT infrastructure (including changes to data structures)
except for major IT projects (e.g., the procurement of multiple new systems and their integration with one another).

The Head of MIS, Compliance & Admin will conduct quarterly reviews to ensure that the Change Management procedure is being complied with and is meeting the practical requirements of the business units.

All changes to system hardware, software, configuration, authorised users, and operating procedures
are to be authorised by the Head of MIS, Compliance & Admin. Any changes are to be reflected in an update to relevant documents.

All security relevant changes will be discussed with the ELA Risk Assurance Team.

Communications and IT Operations Management

The Head of IT Operations 3rd party (or authorised Deputy) shall maintain a secure configuration -controlled set of system documentation. This documentation shall record the current configuration

of the system, including a history of changes together with dates and business justifications. Modifications which are considered by the Head of IT Operations 3rd party (or authorised Deputy) to affect the network security profile shall be accompanied by a written justification for the modification

and will identify all component changes. Changes will be categorised as follows:

a. Security CRITICAL changes.
b. Security SENSITIVE changes.
c. Security NON-SENSITIVE changes.

All proposals of category (a) or (b) will be submitted to the Head of MIS, Compliance & Admin who will make an assessment as to the impact. In the event that it is considered that the proposals will impact the status of the systems, appropriate action will be taken to ensure the security related aspects of the proposal are addressed.

The Head of MIS, Compliance & Admin may seek any additional advice from external 3rd parties.

7.3 Segregation of Duties

Where practical, duties will be segregated to reduce opportunities for unauthorised or unintentional

modification or misuse of ELA's information assets.

No single person will be solely in control of the initiation, authorisation, and completion ("acceptance")

of a process or procedure where there could be the opportunity for modification or misuse intentionally or unintentionally.

7.4 Separation of Development, Test and Operational Facilities

Development, test, and operational facilities will be separated to reduce the risks of unauthorised access or modification to the production environment.

7.4.1 Procedure for the Management of Test and Development Facilities and Processes

All development and testing of software within ELA will be performed on dedicated systems that are

separate from all operational and production software and data.

The development and test environment should be treated as untrusted from a security perspective. Protected and restricted data should not be copied into the development and test environment. However, subject to this requirement, test data should always be as realistic as possible.

To minimise the risk of accidental confusion between the operational and the test / development domains, users should use different user profiles for accessing operational and test / development systems.

7.5 Third Party Service Delivery Management

Where IT Partners / 3rd Parties are providing services (e.g., Infrastructure, network, and capacity monitoring etc.) that could impact on the confidentiality, integrity, or availability of ELA's systems and data, the services and required performance levels (SLA's) will be documented and agreed with the third party involved.

The performance of the third party (and particularly their compliance with SLA's and relevant information security policies and procedures) will be monitored and, where deemed appropriate by the Head of MIS, Compliance & Admin, compliance audits will be conducted on a regular basis.

7.6 Protection Against malicious and Mobile Code

Computer viruses and other forms of malicious code (collectively referred to as "malware") are to be regarded as a serious and likely threat to ELA 3rd party IT infrastructure.

ELA and its 3rd party IT provider will therefore establish a series of controls that ensure appropriate anti-virus software is implemented and maintained at each level within the network (gateway, server,
desktop, laptop, mobile device).

7.6.1 Procedure for the Selection and Administration of Anti-Virus Software

ELA's 3rd party IT provider selected standard anti-virus software shall be installed on all of the appropriate servers, desktops, laptops, and mobile devices (tablets and smartphones for example). The software will be kept up to date, and automatic scanning for viruses should be activated whenever such equipment is in use. Changes to the standard anti-virus software may only be made with the explicit agreement of the Head of MIS, Compliance & Admin.

The IT Department / 3rd Party IT Provider shall on a regular basis (at least annually) review the performance of the anti-virus software vendors and, if necessary, recommend a change of vendor.

Virus definition files are to be obtained from the vendor daily and all devices connected to the network updated within four hours using a suitable automated software tool.

It is recognised that the automatic roll out of new anti-virus signature files may not be possible in the
case of devices that are periodically disconnected from the network. These devices are to be updated

by an Internet connection or as soon as they are connected to the network. This must be enforced through automated processes. Remote systems should be configured to download signatures daily from the vendor website.

Whenever any visitor is given access rights to the network the IT Department shall ensure that an acceptable up to date version of Anti-Virus software is installed on that visitor's computer prior to access being granted.

Files that enter ELA 3rd party IT provider network, for example by e-mail or USB stick, must be scanned by antivirus controls. When it is not possible for the device holding the file to have antivirus installed, the file must be copied as soon as possible to a device that runs antivirus software and the file scanned.

The IT Department shall on a weekly basis audit the currency of the anti-virus software installed on all computers accessing ELA network. This weekly audit shall comprise the following steps:

- Review the administrator interfaces to the anti-virus software tools in use, and check that the signatures are up to date and are being pushed out.
- Select one server, one workstation and one gateway device at random to check that the anti-virus software that they are running is up to date.

7.6.2 Procedure for Managing Malware Incidents

In the event of the 3rd party IT Department becoming aware of an actual or suspected virus infection of any ELA IT Asset, this shall be reported straight away as a security incident, using the incident management process through the 24/7 Service desk to the Head of MIS, Compliance & Admin, or authorised deputy.

Appropriate measures shall be taken immediately to contain and eliminate the infection, and to investigate any possible spread of infection that may have already occurred. As a minimum, the following steps shall be taken:

- All users of (actual or suspected) infected computers shall be instructed to shut down their computers immediately.
- The IT Department shall run a comprehensive virus scan on those machines once they have been disconnected from the network.
- If deemed appropriate by the Head of MIS, Compliance & Admin (or designated nominee), the anti-virus software vendor shall be contacted, and advice sought.

7.6.3 User Responsibilities for Anti-Virus Protections

All users of ELA network (including visitors with network access) are responsible for ensuring that:

- They do not introduce a virus from an external source into ELA network.
- When using ELA IT Assets, the equipment that they are using is running the most current version of ELA approved (AV) anti-virus software.
- They report any suspicious incidents relating to malicious software immediately to the IT Department by (in the first instance) contacting the Service Desk.
- They follow any instructions received from the IT Department regarding dealing with a virus threat.

Users of ELA IT Assets can meet their personal responsibility to play their part in protecting against malicious software by observing the following guidelines:

- Never open any files or macros attached to an e-mail from an unknown, suspicious, or untrustworthy source. Delete these attachments immediately, then "double delete" them by emptying your Recycle Bin or Trash. Users to contact IT/Service Desk if further information/assistance id required.
- Delete spam, chain, and other junk e-mail without forwarding.
- Never download files from unknown or suspicious sources.
- If for whatever reason the anti-virus software on your computer is disabled, do not run any applications that could transfer a virus, e.g., e-mail or file sharing whilst that disablement is current and contact the IT Department before continuing to operate the computing device.
- The IT Department shall from time-to-time issue e-mails to all users alerting them to new virus threats. When you receive such an e-mail, read it as a matter of priority and ascertain what action (if any) you need to take. If you have any doubts, contact the Service Desk.
- Never forward an e-mail containing advice on viruses or vulnerabilities that has not been received from the IT Department, as this may be a hoax. When in doubt, contact the Service Desk for advice.
- Always comply in full with any instructions or advice received from the IT Department regarding threats or occurrences of viruses / malicious software. Failure to do so could seriously jeopardise the availability and security of the ELA network.

7.6.4 User Responsibilities for Mobile Code

All users of the ELA network (including visitors with network access) are responsible for ensuring that Mobile code, such as ActiveX, Java, JavaScript, VBScript, MS Word macros and PostScript is not installed or downloaded onto ELA assets.

If there is a legitimate business reason to install mobile code a request should be made to the IT Department/Service Desk in writing/email.

7.7 Availability Monitoring and Management

ELA implements a uniform approach to detection of all availability issues across its 3rd party provided IT infrastructure.

A centralised systems availability and monitoring tool could be deployed throughout the virtual ELA IT infrastructure. This tool monitors all 3rd party IT server systems and all networking devices.

On being notified of a potential availability issue, the IT Department shall perform a brief risk assessment, and determine an appropriate action path.

This risk assessment should include a rating of any security risks implied as a result of the service unavailability, and a rating of the relative significance of that system to ELA's business operations.

The results of this assessment may lead the IT Department to decide to restart the system the next business day, or immediately.

The Head of IT Operations 3rd party (or their nominee) shall investigate any continued availability problems. Whilst the first priority must always be to restore the service as soon as possible, consideration must also be given to ensuring that availability problems are avoided in the future. Any newly identified risks should be added to the Risk Register.

7.8 Backup and Data Restoration

Protection against loss of data and data restoration is managed primarily within the context of the Business Continuity Plan (BCP).

However, in addition to the data replication and restoration procedures associated with the BCP, data will also be backed up to a secure off-site location.

The Company provides back-up facilities for data stored on its servers/3rd party partners servers. Users or departments requiring access to space on a server for storage of data are allocated a private folder for this purpose. Data saved on local drives (C:\ for example) or desktops is not automatically backed-up and it is the user's responsibility to ensure to ensure this is periodically copied to a private folder on a server.

Backed up data will be tested periodically the IT Department.

7.8.1 Backup Process

Recovery of data is primarily addressed by alleviating the need for conventional recovery through an "active / active" approach (i.e., with an active recovery site as well as an active production site).

As a second line of backup, a daily snap will be made of all servers and replicated to the recovery site.

A quarterly full back up to an offsite facility will also be made and stored for a minimum of 12 months.

The Head of IT Operations 3rd party will monitor the backup process and, in particular, will check that each quarterly backup has been successful reporting to outcome to the Head of MIS, Compliance & Admin.

7.8.2 Procedure for Backup Testing Process

The effectiveness of the backup will be tested.

The Head of MIS, Compliance & Admin will make spot checks on an annual basis to check the integrity of the quarterly backups.

7.8.3 Procedure for Data Archiving Process

Email and file archiving will be concurrently managed by an archiving product approved by the Head of IT Operations.

Any files that are not accessed for 12 months will be archived / securely stored off system-Network prior to permanent deletion.

7.9 Secure Disposal

Hard disks must be cleared of all software and all organisational protected and restricted information prior to disposal or reuse.

In the event that hard disks/media contain personal data, and it cannot be removed, then:

- Review whether or not you really do need to keep an archive within which this personal data is stored; it may well be that there is no overriding business reason for the archive in the first place.
- If you currently cannot technically delete archived data that is beyond its retention date, then the hard disk/media needs to be stored securely out of use.

The Information Asset Owner is responsible for the secure disposal of storage media and the disposal of all information processing equipment relating to the information asset they are responsible for. A log will be retained showing what media was destroyed and/or disposed of, and when. The information asset inventory and/or data inventory is adjusted once the asset has been disposed of.

Devices containing protected and restricted information are destroyed prior to disposal and are never reused.

Devices containing protected and restricted information that are damaged are subject to a risk assessment prior to sending for repair, to establish whether they should be repaired or replaced.

Portable or removable storage media of any description are destroyed prior to disposal.

Documents containing protected and restricted information that are to be destroyed are shredded by Employees. The shredded waste is stored in a secure waste bin which is removed by the approved ELA 3rd Party data sanitisation contractor.

7.10 Management and Configuration of Servers

The Head of IT Operations will ensure that all ELA server equipment is managed and configured.

Designated IT personnel qualified for system administration approved by the Head of IT Operations 3rd party must manage servers in compliance with these requirements.

7.11 Management and Configuration of Routers, Switches and Firewalls

The Head of IT Operations will manage other approved select 3rd Party IT partners to ensure that all applicable Router, Switch and Firewall devices are supported, configured, and documented.

Designated 3rd party IT personnel qualified for system administration approved by the Head of MIS, Compliance & Admin must manage Router and Switch devices in compliance with these requirements.

ELA can use Windows Authentication and Active Directory accompanied with group policies to protect files and folders from unauthorised access.

In future ELA may adopt to use VLANs to segment the network. If a physical separation of the network is required, this is done at the switch level ensuring that it is not possible to bridge the two networks.

Any Switches, Routers and Firewalls are controlled by IT only and it is not possible to reconfigure them unless the individual is authorised to do so. These pieces of equipment are physically stored in locked rooms where only authorised IT staff are permitted to enter.

The MS Windows Network authentication process can be used on the ELA Client/Server network. The computers can be identified by a standard naming convention consisting of the Asset Tag number.

7.12 Wireless Computing

Wireless access to ELA network is available to all authorised staff.

Wireless connectivity may only be established for a user in accordance with the requirements set out in this section.

Designated IT personnel qualified for system administration approved by the Head of MIS, Compliance & Admin must manage wireless access in compliance with these standards.

7.12.1 Wireless Computing Standards

- Authentication of wireless users shall be achieved through enterprise authentication to Active Directory via a RADIUS server.
- All wireless access points and base stations shall be subject to periodic penetration tests on a minimum of an annual basis.
- Data is to be encrypted with a standard secure algorithm.

The 3rd party provider IT Department is responsible for ensuring this policy is applied to all wireless connections.

7.13 Exchange of information

7.13.1 Information exchange policies and procedures

ELA shall ensure that formal information interchange policies, procedures, and controls shall be in place to protect the exchange of information through the use of all types of communication facilities.

7.13.2 Exchange agreements

Agreements shall be established for the exchange of information between ELA and external parties to ensure the confidentiality, integrity and availability of information (C,I,A).

7.14 Audit Logging

Details of security related events are recorded. The events are recorded under two categories -

1. Security violations and security related events.
2. Attempted security violations include failed attempts to 'access' a system’s functions.

Security related events include the following:

- Logon and Logoff (success / failure),
- File and Object Access (failure),
- Change to User Rights (success / failure),
- Remote access using both dial-up and VPN connections (success / failure),
- Detection of malicious code,
- Clearing down of the event log.

The firewall software shall log traffic over the connections to external systems and alerts the Administrators of any attempted violation of policy. Access logging shall be used to enable the Administrators to investigate any incident.

The following records are to be requested from the 3rd party IT partner/administrator and maintained by the Head of IT Operations. These records are maintained using operating system procedures where practicable and do not imply that a hard copy record is maintained:

- Computer Log – register of all successful and unsuccessful logon attempts (including those made by the remote access facilities).
- A record of all authorised users and their privileges.
- Register of staff with system administrator access privileges.
- Firewall Log – record of all attempts to violate the policy implemented by the Firewall.

Logs are to be reviewed on a monthly basis by the Head of IT Operations who reports any anomalies as a matter of urgency to the Head of MIS, Compliance & Admin as a security incident and documents them in the monthly IT Management Report presented to the Executive Committee.

Logs are protected by preventing unauthorised access to systems via passwords and active directory.

7.15 Clock Synchronization (Network)

ELA shall maintain a full synchronized timing system throughout the whole of the network.

An Internet accurate time shall be identified and used as the master time source.

7.16 Fault Logging

ELA shall install and maintain a mechanism for the tracking and monitoring of reported faults.

All faults are reported to the IT Department and recorded in the Service Desk Software.

Access Control

8.1 Overall Approach to Access Controls

ELA is committed to implementing and maintaining strong access controls to prevent unauthorised access to its systems and data, whilst simultaneously ensuring that all users have levels of access consistent with their needs in order to carry out their duties efficiently.

ELA's access controls have both an "internal" and "external" focus. Internal controls for authenticated users are driven by the "principle of least privilege": however, the associated procedures also need to be sufficiently flexible to enable changes to be made to a user's access privileges rapidly and efficiently to meet the needs of a dynamic working environment.

External controls aimed at preventing malicious 3rd Parties gaining access to ELA's systems and data are achieved through strong authentication procedures.

Working in conjunction with the HR Department the Head of MIS, Compliance & Admin has overall responsibility for ensuring effective access controls. In discharging this responsibility, the Head of MIS, Compliance & Admin will:

- Ensure that standard user access controls are managed according to the principle of least privilege, whilst not impeding users in performing their roles within ELA.
- Ensure that privileged access for members of the IT Department, internal and 3rd party IT provider, is managed in a way that minimises the risk of security incidents occurring.
- Implement effective controls in regard to remote access.
- Ensure that strong passwords are used throughout ELA and that users are aware of the importance of protecting their passwords against misuse by 3rd Parties.
- Implement appropriate network segmentation.

8.2 Log-in and Password Controls

All users with access to any of ELA IT infrastructure shall be uniquely identified and authenticated via unique user accounts and passwords. Only strong passwords may be used, and these will be changed at regular intervals.

Special rules apply in the case of log in and password controls for privileged access.

All computers left on that are inactive for more than 3 minutes shall automatically lock until the user enters a valid password. Areas where there are sufficient physical controls or the disruption to the business is possibly deemed too intrusive, a risk assessment will be conducted, and the outcome entered into the Risk Register.

Failed or unauthorised user access attempts will be logged and monitored and investigated accordingly.

The IT Department shall manage the overall processes of log in and password control in accordance with the procedure Log in and Password Management.

The Head of IT Operations will conduct quarterly audits of password controls and report any findings to the Head of MIS, Compliance & Admin.

8.2.1 Procedure for Log in and Password Management

Log in and password controls are central to the security of ELA, and the IT Department shall manage the overall processes of logging in and password control in accordance with the following procedures:

- All users with access to any of ELA infrastructure shall be uniquely identified and authenticated via unique user accounts and passwords.
  - Generic accounts for shared computers are permitted provided the strict controls have been placed around Internet access and other potential attack vectors. A risk assessment must be performed, and the outcome placed on the Risk Register.
- Users shall be permitted only one user account per system, and (where appropriate) only one admin user account per system.
- User profiles and password files shall at all times be protected from unauthorised additions, modifications, viewing or removal.
- Users shall only be permitted three access attempts before their accounts are disabled (Prior to the resetting of a disabled user account, the IT Department shall review the reasons why this event transpired and shall verify the identity of the user).
- Users shall change their passwords whenever there is a suspected security compromise.
- A system-controlled password history file shall be maintained in order to prevent users from reusing old passwords.
- New accounts shall be assigned default passwords that are different to the username. Users shall immediately change their passwords once they have been assigned a new password (this shall be enforced by the system).
- All access attempt violations shall be logged and periodically reviewed by the Head of IT Operations (at least quarterly), and any suspicious violation shall be investigated and reported to the Head of MIS, Compliance & Admin.
- All computers left on that are inactive for more than 3 minutes shall automatically lock until the user enters a valid password. Where password screen savers or other security utilities cannot be used, users shall log off or lock their systems before they leave their computer.
- All system-level passwords must be changed on at least a Quarterly basis
- All user-level passwords (e.g., e-mail, desktop computer, etc.) must be changed at least every 90 days.
- The IT Department shall ensure that wherever possible, system settings are configured to reject weak passwords being registered by users

8.2.2 Password Compliance Audits

The annual compliance review conducted by the specialist information security partner shall include an audit of compliance with this Policy.

8.2.3 User Responsibilities for Passwords

All users have an individual responsibility to ensure that security is not compromised by any failure on their part to manage their passwords securely. Users shall comply with the requirements set out in User Password Management Responsibilities.

8.2.4 User Password Management Responsibilities

- Passwords are to be changed on a regular basis; this will be enforced by the network operating system.
- Password creation under best practice should be at least 8 characters in length and unrelated to any aspect of your personal life e.g. do not use wife's name or mother's maiden name.
- Users must not write passwords down.
- Passwords and related guidelines must be used at all times to gain access to any of the Company's personal computers. Do not give your personal password to anyone else, except in very exceptional circumstances, where you should obtain agreement from your Line Manager. If you suspect that your password has been compromised, you should contact The IT Department immediately.
- The system will prompt the user to change passwords at regular intervals not exceeding 90 days.
- Users are permitted to create their own passwords. The following general provisions shall be adhered to.
    - Users should generate unique passwords.
    - Passwords should not be based on the following:
- Months of the year, days of the week or any aspect of dates with which they are personally associated (e.g., birthdays, anniversaries etc).
- Family names, initials, or car registration numbers.
- Organization names, identifiers, or references.
- Telephone numbers or similar all-numeric groups.
- User ID, username, group id or other system identifier or job-related title.
- Any other guessable personal characteristic (e.g., address, nickname, favourite team, etc).
- More than two consecutive identical characters.

Users shall ensure that:

- Passwords are changed at regular intervals.
- Passwords are changed as soon as possible when a compromise occurs.
- Passwords are not recycled.
- Temporary Passwords are changed at first logon.
- All default vendor-supplied system Passwords on installation of software are changed as soon as possible.
- Passwords are stored securely.

Users must not:

- Tell anyone else his or her Passwords.
- Allow anyone to watch when entering them.
- Allow them to be printed out.
- Allow them to be written down and stored in an insecure way.
- Disclose them in any other way.
- Use the same Password on two different systems.

8.2.5 Resetting Lost Passwords

From time-to-time users lose or forget their passwords. When this occurs, it is particularly important that the IT Department ensures the identity and validity of the user before issuing a new password.

8.2.6 Process for Resetting Lost Passwords

When a password needs to be reset, the IT Department shall act in accordance with the following procedures:

- When a user loses or forgets their password, they shall contact the IT Service Desk, who will check to ensure that the user's access account has not been disabled in the Active Directory.
- The IT Service Desk shall then verify the identity of the caller.
- If the IT Service Desk is satisfied that the request is valid, they will issue that user with a unique (i.e., different every time) one-time random password that will auto expire the next time the user logs on, thereby obliging the user to create a new password.
- The IT Service Desk will inform the user that they are required to log on and change their password within two hours of the password having been re-set.

8.2.7 Setting Up New User Accounts

Prior to any new user being granted access to ELA network (whether that user is a permanent employee, a temporary member of staff, or an external contractor), a new user account will be established.

The user account will reflect the access rights necessary for that employee to carry out their role within the organisation. These rights shall be determined by the user's manager by completing a User Account Form.

New user accounts will only be activated by the IT Department once the User Account Form has been received and verified, and once the HR Department has confirmed that the new user has satisfied all pre-employment requirements.

8.2.8 Review and Modification of User Accounts

User accounts may be modified as necessary to reflect changes to the user's role and responsibilities, or changes to the IT infrastructure (e.g. new applications becoming available for users).

Users' access rights will be reviewed by the Head of IT Operations on a 6-12 monthly basis or after any changes are made in the system, structure, or an individual's role. This will include privileged user accounts.

8.2.9 Terminating User Accounts

User accounts will be terminated using a two phased approach in accordance with the procedure below.

The HR Department will co-ordinate with the IT Department to ensure the effective implementation of this procedure.

Initially the account will be disabled immediately the user's employment or engagement is terminated. The account will remain disabled for 3 months after which the account will be permanently deleted.

The Head of IT Operations will conduct spot checks at six monthly intervals to ensure that this Policy is being complied with and notify the HEAD OF MIS, COMPLIANCE & ADMIN of any non-conformances.

8.2.10 Procedure for the Termination of User Accounts

User access to ELA network is to be discontinued immediately when an employee leaves or a contractor, temporary member of staff or visitor completes their assignment.

The following procedures shall apply:

- The IT Department shall disable a user's access rights when HR or the user's manager (for contractors or temporary staff only) notifies the IT Department by e-mail. This shall occur immediately when an employee leaves or a contractor, temporary member of staff or visitor completes their assignment.
- A confirmation e-mail of the removal of the account will be sent by the IT Department to Human Resources and the user's manager.
- The IT Service Desk will ensure that a user's access rights are disabled on the date required by the manager submitting the request. This should be accomplished by resetting the password immediately. Where the user has a mailbox, this will be set to the "Out of Office" automatic reply for 30 days following the user's departure. The exact content for the 'Out of Office' auto- reply is to be provided by HR or the user's manager.
- Three months following the disablement of a user's access rights the user account will be fully terminated by the IT Department. At this time, the following shall occur:
  - o The log in rights associated with that account shall be fully removed.
  - o All files in that user account shall be archived.
  - o The e-mail boxes associated with that user account shall be removed, and the contents shall be archived.

8.2.11 Emergency Access to User Accounts

Emergency access to another user's account is only to be provided when access is required to that user's documents or e-mail account in a genuine emergency and when the account owner cannot provide access to the required resources in an acceptable time frame (due to sickness, leave etc).

Any such emergency access is subject to strict controls and may only occur in accordance with the procedure below.

8.2.12 Procedure for Emergency Access to Other Users' Accounts

The following procedures shall apply:

1. When a user requires access to another user's resources, they should contact the IT Service Desk.
2. The IT Service Desk will identify the user making the request and confirm with the user via email. The user must provide the line managers name, the reason for the request and length of time access is required.
3. The IT Service Desk will then confirm with the account owner's manager that the access has been requested and seek written approval.
4. Once received the line manager will approach HR requesting approval.
5. HR will notify the IT Service Desk approving the access request.
6. On their return, the account owner will be notified by the IT Service Desk of the emergency access that occurred.

8.2.13 Privileged User Accounts

In order to ensure efficient administration of ELA's 3rd party supported IT infrastructure, it is necessary for members of the IT Department to have additional access rights beyond those of a normal user. This is known as "Privileged Access".

In consultation with HR the Head of IT Operations will establish and manage a series of Roles for members of the IT function. For each role there will be a set of defined privileged access rights.

All privileged roles and access rights will be documented in the Privileged Roles Record to be maintained by the Head of IT Operations who shall ensure that the record is always current.

Changes to this record may only be made by the Head of IT Operations who shall also notify the HR Department and Head of MIS, Compliance & Admin of such changes.

Staff granted privileged access will exercise that access strictly in accordance with the requirements set out in the procedure below relating to passwords and usage.

Information Systems Acquisition, Development and Maintenance

9.1 Security requirements of information systems

Staff shall request new business requirements and shall include any specific requirements for security.

The ELA Risk Assurance Team shall review all such requests in relationship to current security policy.

ELA operate from a preferred supplier list all of which have been subject to due diligence and a business case for each purchase must exist before the purchasing process can be followed.

The Head of MIS, Compliance & Admin must authorise the procurement of a new Information System and ELA Risk Assurance Team must authorise its use.

9.2 Security of system files

9.2.1 Control of operational software

The installation of software onto any ELA asset shall be strictly controlled.

9.2.2 Access control to program source code

System source code shall only be held on ELA development system.

No source code shall be permitted on the main ELA corporate network.

All source code shall be held within the development system to which there is not access from the outside.

9.3 Technical Vulnerability Management

Vulnerabilities (as used in the context of this Policy) are known weaknesses in commercially available software that can be exploited by hackers and malicious software so as to cause damage to or gain unauthorised access to ELA's Information Assets.

The Head of IT Operations is responsible for co-ordinating the 3rd party IT provider for vulnerability and patch management so as to ensure that ELA's IT Assets are not harmed through the exploitation of any new vulnerability. The IT Department will manage this process through the monitoring of new vulnerabilities and patches, assessing the risk associated with vulnerabilities, planning testing, and implementing patch rollout, and auditing ELA's systems for unpatched hosts.

Vulnerability and Patch Management covers all software including applications and operating systems running on desktops, thin clients, servers, and network devices such as routers firewalls and switches.

9.3.1 Procedure for Monitoring Vulnerability Information Sources

New vulnerabilities are identified by global information security monitoring organisations on a daily basis. When a new vulnerability is announced, it is usual for a corresponding patch (or update) to be announced simultaneously. [Note that for the purposes of this policy statement, the term “patches” will be deemed to include upgrades, hot fixes, and similar responses to vulnerabilities].

The Head of IT Operations shall designate a member of the IT Department to be responsible for ongoing daily monitoring of new vulnerabilities and their associated patches. This individual should have specialist knowledge in monitoring new vulnerabilities, identifying new patches and updates, and assessing risk and priorities.

Sources of information regarding new vulnerabilities and patches will be checked on a daily basis.

9.3.2 Procedure for Vulnerability Risk Assessment Process

For every new patch that is identified as being relevant to ELA infrastructure, an assessment of the level of risk of the associated vulnerability must be made. This assessment is made with a consideration of all the surrounding circumstances.

9.4 Testing of New Systems

New systems will be tested fully prior to implementation in the production environment. Data will be used that is as close as possible to true operational data but not ‘real’ data that is classified as protected or restricted

In the case of Internet facing applications, these will be subjected to a security code review process by a suitably qualified third party prior to deployment.

About this document

Content Owner: Farhan (Fuz) Zaidi, - Head of MIS, Compliance & Admin	**Owning Team:** Executive
For further information, please contact: Farhan (Fuz) Zaidi - Head of MIS, Compliance & Admin	