Access Control Policy

IGDP_P7 VERSION 1.00

ELOPSIS ELECTRONIC OPTRONIC DEFENSE SYSTEMS CORPORATION

Access Control Policy

1. Purpose and Scope

ELOPSIS implements physical and logical access controls across its networks, IT systems and services in order to provide authorized, granular, auditable and appropriate user access, and to ensure appropriate preservation of data confidentiality, integrity and availability in accordance with our Information Security Policy

Access control systems that we have put in place aims to protect the interests of all authorized users of Company controlled IT systems, as well as data provided by third parties, by creating a safe, secure and accessible environment in which to work.

1.1. Provisions of this Policy apply to all data, information and systems owned or operated by ELOPSIS at all locations with access to company's corporate systems. They cover all vendors, contractors, subcontractors, consultants, sub-consultants, volunteers, individuals doing research, student interns, temporary employees, and other persons including those Users affiliated. Throughout this Policy, the words Users and User shall be used to collectively refer to all aforementioned individuals including third parties and other organizations that are granted authority to access data, information and systems controlled by ELOPSIS.

1.2. The ELOPSIS external corporate website and other information classified as 'Public' are considered as outside our control and will not fall under this Policy. Privileged access to non-ELOPSIS controlled systems, resources and applications is the responsibility of the system, resource or application owner, *not* ELOPSIS. The authorisation and auditing processes involved in granting access to these resources is the responsibility of the resource owners.

2. Definitions and Roles of Participants

2.1. Access to data, information and systems will be granted only when a legitimate business need has been demonstrated, access has been approved in advance by the Information Technologies Supervisor, and all applicable policies, procedures and requirements have been complied with. When a User no longer has a need for system access by reason of job reassignment, retirement, termination of contract, end of project, etc. all system privileges must cease, and access to information must likewise cease.

2.2. User privileges must be defined so Users cannot gain access to, or otherwise interfere with, the individual activities of other Users or any data that the Information Technologies Supervisor has not specifically authorized access to for that User.

2.3. Least privilege and need to know principles: Access rights to both physical and logical assets will be accorded following the principles of least privilege and need to know.

2.4. **Least Privilege Principle**: The principle of least privilege requires that a User be given no more privilege than necessary to perform an authorized job or task. Ensuring least privilege identifying what the User's job is, determining the minimum set of

privileges required to perform that job, and restricting the User to those privileges and nothing more. Privileges should be granted only for the timeframe required for the job. The principle of least privilege will be employed requiring that access control permissions for all systems must be set to a default which blocks access by unauthorized Users, and every information system privilege which has not been specifically allowed is forbidden.

2.5. **Security in Depth**: The principle of security in depth refers to the implementation of a security defense in multiple layers of different types to provide substantially better protection. The principle of security in depth will be employed requiring access control at each layer of the system including network, hardware devices, system software, applications and data.

2.6. **Separation of Duties**: Whenever a business process involves sensitive or critical information, the system must include controls involving a separation of duties or other compensating control measures. These control measures must ensure that no one individual has exclusive control over these types of information assets or functions related to them. An example of a lack of separation of duties is where a single person has control of issuing checks and maintaining the financial transaction history data. Whenever practical, no person should be responsible for completing a task involving sensitive or critical information from beginning to end. Likewise, a simple person must not be responsible for approving his or her own work. To the extent possible, for every task at least two people must be required to coordinate their information-handling activities.

2.7. **Acceptable Use Policy**: All Users requiring authorization to use ELOPSIS data, information and systems that are connected to ELOPSIS internal networks will be notified of Acceptable Use Policy of IT and Electronic Resources and required to sign Information Security Awareness Declaration prior to being issued a user-ID.

2.8. **Non-Disclosure of Information**: All outside parties with access to company data, information and systems must refrain from disclosing any information deemed non-Public by ELOPSIS. For outside parties employed under a contract, purchase order, or agreement, a standard Information Security Confidentiality Clause will be included in all agreements, contracts, and purchase orders between ELOPSIS and the outside party being granted access to ELOPSIS data, information and systems. A written Non-Disclosure Agreement will be used for all individuals or entities that are providing services to ELOPSIS (requiring access to confidential data) but are not under contract with ELOPSIS. Examples of persons providing services to ELOPSIS who are not under contract would include student interns, volunteers, instructors, academicians, guest speakers, and members of professional organizations.

2.9. **Access Control**: Access control is any mechanism to provide access to data. For computer access, a User must first log in to a system, using an appropriate authentication method. The access control mechanism controls what operations the User may or may not perform by comparing the user-ID to an access control list. Access control systems include the following:

- File permissions, such as create, read, edit or delete on a file server
- Program permissions, such as the right to retrieve or update information in a data base

- Right to make changes to data, such as retrieving data from a database or updating information.

Access control procedures are the methods and mechanisms used by Information owners to approve permission for Users to access data, information and systems.

2.10. **Authentication**: Authentication is the process of identifying an Information User by the user presenting credentials. In a computer system, this is most often accomplished by using the unique user-ID and password combination which is assigned to and known only by the Information User. Other techniques of authentication may be employed with the approval of the Chairman of the Executive Board upon the proposal submitted by the Information Technologies Supervisor or Security Coordinator.

2.11. **System:** A system shall be defined as an interconnected set of information resources under the same direct management control that shares common functionality. System may include hardware, software, information, data, applications or communications infrastructure.
A production system is a system that is used to process information or support on-going business functions. Information systems which have been designated production systems have security requirements defined that are based on the business need.

2.12. **Individual Accountability**: Individual accountability is required when accessing all electronic resources provided by the ELOPSIS. Access to computer systems and networks must be provided using individually assigned unique computer identifiers, known as user-IDs. Individuals who use our corporate computer resources must only access resources to which he or she is authorized. Associated with each user-ID is an authentication token, such as password, which must be used to authenticate the person accessing the data, information and system. Passwords must be treated as confidential information, and must not be disclosed. Each individual is responsible to reasonably protect against unauthorized activities performed under their user-ID. For detailed information please refer to Directive on Principles and Code of Conduct for User Passwords.

2.13. **Information Asset Owners**: Information Asset Owners are responsible for determining who should have access to protected resources and what those access privileges will be (read, update, etc.) These access privileges will be granted in accordance with the Information user's job responsibilities. Information Asset Owner may delegate administrative responsibility but are ultimately accountable for the information asset they own.

2.14. **Department Chiefs**: Department Chiefs have a pivotal role in the security of ELOPSIS information. It is the responsibility of Department Chiefs to document and request system access on behalf of Information Asset Owners when access is required in the performance of duties. It is the responsibility of the Department Chief to request the user's access be revoked in the event of a change in job responsibilities or status of an Information user.

2.15. **Information Security Liaison Officers**: Information Security Liaison Officer serves as a primary point of contact between their office and Information Technologies Supervisor and Security Coordinator. These responsibilities will be fulfilled by each Chief of Department and Director of Abroad Facility. Information

Technologies Supervisor may also be assigned as Liaison Officer. Information Security Liaison Officers shall validate requests for User access to data, information and systems from supervisors or managers and authenticate the requestor. Information Security Liaison Officers will also provide information security support for their constituents and provide feedback to the Security Coordinator regarding problems with policy and security issues.

3. Procedural Guidelines Regarding Access Control

3.1. ELOPSIS will provide all employees and contracted third parties with on-site access to the information they need to carry out their responsibilities in as effective and efficient manner as possible.

3.1.1. **Generic Identities**: Generic or group IDs shall not normally be permitted as means of access to ELOPSIS data, but may be granted under exceptional circumstances if sufficient other controls on access are in place.

3.1.2. Under all circumstances, users of accounts must be identifiable in order for ELOPSIS to meet the conditions of its Internet Service Provider and pursuant to MSY 317-2 (C) Communiqué on Security of Defense Industry (as laid out in the 'Acceptable Use Policy'). Generic identities will never be used to access Confidential data or Personally Identifiable Information.

3.1.3. **Privileged Accounts**: The allocation of privilege rights (e.g. local administrator, domain administrator, super-user, root access) shall be restricted and controlled and not provided by default.

3.1.3.1. Authorization for the use of such accounts shall only be provided explicitly, upon written request from a senior manager (such as Information Technologies Supervisor or the Security Coordinator), and will be approved by the Chairman of the Executive Board and documented by the system owner.

3.1.3.2. Technical teams shall guard against issuing privilege rights to entire teams to prevent potential losses of confidentiality and / or integrity.

3.1.3.3. Privileged accounts must not be used for standard activities; they are for program installation and system reconfiguration, not for program use, unless it is otherwise impossible to operate the program.

3.1.4. **Least privilege and need to know**: Access rights to both physical and logical assets will be accorded following the principles of least privilege and need to know

3.2. Access Control Authorization

3.2.1. **User Accounts**: Access to ELOPSIS IT resources and services will be given through the provision of a unique user account and complex password.

3.2.2. Accounts are provided on the basis of valid records in the Human Resources. For any user not in either of those systems, access is granted via the appropriate staff or associate form signed by a Head of Department of Departmental manager. Default access is granted only to a specific space, a storage medium and an email account.

3.2.3. **Access to Confidential, Restricted and Internal Use Information**: Access to 'Confidential', 'Restricted' and 'Internal Use' information will be limited to authorized persons whose job or study responsibilities require it, as determined by law, TOGEK, contractual agreement with interested parties or the Information Security Policy. Access to any of these resources will be restricted by use of

firewalls, network segregation, secure log-on procedures, access control list restrictions and other controls as appropriate. The responsibility to implement access restrictions lies with the Chiefs of Departments and Information Technologies Supervisor, but must be implemented in line with this policy. Role-based access control (RBAC) will be used as the method to secure access to all file-based resources contained within ELOPSIS's Active Directory domains and administered by ELOPSIS. There are no restrictions on the access to 'Public' information.

3.3. **Authentication and Identification**: All computers connected to the Company's network must have an authentication mechanism such as a user-ID and password for access control. Multi-user systems must employ user-IDs and passwords unique to each User, as well as User privilege restriction mechanisms. All workstations whether connected to the network or not, must employ hardware or software controls approved by the Information Technologies Supervisor and implemented by the system administrator that prevent unauthorized access.

3.4. All Users must be positively identified prior to being able to use any data, information or system. Positive identification for internal networks involves both a user-ID and a password, both of which are unique to an individual User.

3.5. Users must not use the same user-ID or password that they use for access to ELOPSIS systems and information to access non-ELOPSIS systems, including any internet accounts.

3.6. The log-in process for network-connected computer systems must simply ask the User to log-in, providing prompts as needed. Specific information about the organization managing the computer, the computer operating system, the network configuration, or other internal matters must not be provided until a User has successfully provided both a valid user-ID and a valid password. Ig any part of the log-in sequence is incorrect, the User must not be given any information about the source of the problem but simply be informed that the attempt failed.

3.7. **Unique User-IDs**: Each user-ID must be unique and forever connected solely with the User to whom it was assigned. After a User is removed, there must not be any re-use of the invoked user-ID. Every user-ID and related password is intended for the exclusive use of a specific individual. While user-IDs can be communicated in electronic mail messages and in other places, passwords must never be shared with anyone (IT support staff have their own access privileges and will never need to obtain a User's password). A User may have more than one user-ID and password combination if access to multiple security systems is required for the User assignments.

3.8. **User Authentication**: All corporate information system user-IDs must have an associated password or a stronger mechanism (such as a dynamic password token) to ensure that only the authorized User is able to utilize the user-ID. Users are responsible for all activity that takes place with their user-ID and password (or other authentication mechanism). Users must immediately change their password if they suspect that it has been discovered or used by another person. Likewise, users must notify the Information Technologies Supervisor if they suspect that these mechanisms have been compromised. User-IDs may not be utilized by anyone but the individuals to whom they have been issued. Users must not allow others to perform any activity

with their user-IDs. Similarly, Users are forbidden from performing any activity with IDs belonging to other Users.

3.9. **Portable Computers and Other Devices**: Portable, laptop, notebook, palmtop, and other transportable computers and other devices must not store, contain or utilize any confidential or sensitive information unless protected by the standard login process as described above. Users are responsible for the physical security of these devices and the protection of information stored on them.

3.10. **Storage Medias**: Whenever non-public information is written to a floppy disk, magnetic tape, smart card, or other storage media, the storage media must be suitably marked with the highest relevant sensitivity classification. When not in use, this media must be stored in a secure location.

3.11. **Remote Printing**: Controls must be in place to prevent confidential or sensitive information from being viewed by unauthorized personnel. The User must ensure that confidential material is printed on a properly secured printer or one attended to by a person authorized to view the material.

3.12. **Sharing or Transmission of Secure Data**: Users must NOT establish electronic bulletin boards, local area networks, FTP servers, web servers, or modem connections to existing local area networks or other multi-user systems for communicating information without the specific approval of the Senior Management. Only designated IT Department staff with special privileges may establish these types of services.

3.13. **Disposal of Equipment and Media**: Before computer storage media is sent to a vendor for trade-in, servicing, or disposal, all sensitive information must be destroyed or concealed according to methods approved by the Security Coordinator.

3.14. **Privilege Suspension and Revocation**:

3.14.1. Information Technologies Supervisor establishes access conventions for the revocation of User access privileges to the data they own. The Information Asset Owner's designee will use these conventions to grant and revoke User privileges on be half of the Information Asset Owner.

3.14.2. Chiefs of Departments must promptly report all significant changes in a User's duties or employment status that result in changes to access privileges using the computer account administration process. For all terminations, a designated unit such as Human Resources must also notify the Information Technologies Supervisor who will monitor the removal of User access to all data, information and systems to assure compliance.

3.14.3. Chiefs of Departments must reevaluate the system privileges granted to Users every twelve (12) months. In the event that access requirements of the user have changed, the relevant Chief of Department must notify the User's access as detailed in the computer account administration process.

3.14.4. When a User leaves, both computer-resident files and paper/manual files must be promptly reviewed by his or her immediate manager to determine who should become the custodian of such files, and/or the appropriate methods to be used for file disposal. The relevant Chief of Department must then promptly reassign the computer User's duties as well as specifically delegate responsibility for the files formerly assigned to that User.

3.14.5. User-IDs which have not seen any activity for a period of three months will have their privileges automatically revoked. Users who come back from an extended

vacation, temporary reassignment or a leave of absence for more than one month must have their manager reestablish their privileges by the relevant Chief of Department.

3.14.6. Session: If there has been no activity on a workstation for twenty (20) minutes, the system must automatically blank the screen and suspend the session. Re-establishment of the session must take place only after the User has provided a valid password.

3.14.7. **Password Management**: passwords, access control lists and other access control information must always be encrypted in storage or when transmitted over networks. Controls must be in place to prevent the unauthorized retrieval and use of stored passwords and access control information.

3.14.8. To allow passwords to be changed when needed, passwords must never be hard-coded (incorporated) into software or applications.

3.14.9. Initial passwords issued to a new User must be valid only for the new User's first on-line session. At that time, the User must be forced to choose another password. This same process applies to the resetting of passwords in the event that a User forgets a password.

3.14.10. All vendor-supplied default passwords must be changed before any computer or communications system is used. This procedure applies to passwords associated with end-user user-IDs, as well as passwords associated with system administrator and other privileged user-IDs.

3.14.11. Users must not share their individually assigned account password with anyone, including their manager or co-workers. Instead, Users must employ mechanisms approved and authorized by the Information Technologies Supervisor to share information such as local server shared directories, electronic mail, internet pages, or floppy disks.

3.14.12. **System Development:** The following standards prevent access to corporate production data by authorized personnel and improve the integrity of applications: There shall be a separation between the production, development, and test environments. This will ensure that security is maintained in a much more rigorous way for the production system. Development and test staff are nor normally permitted to have access to production systems. Only Chiefs of Departments can approve access to production data to developers. Likewise, all production software testing must proceed with sanitized information (i.e. where sensitive information is replaced with dummy data). A formal and documented change control process must also be used to restrict and approve changes to production systems and information.

Application Development: Prior to moving software to production status, programmers and other technical staff must remove all special access paths so that access may only be obtained via normal secured channels. This means that all trap doors and other short-cuts that could be used to compromise security must be removed. Likewise, all system privileges needed for development efforts, but not required for normal production activities, must be removed. All the User-level and administrative level access controls required by information security policies and procedures must be established and enabled before production information systems can be replaced into operation.

Migration: A methodology must be implemented for an orderly and controlled migration of software from the development environment, through the test environment and ultimately to the production platforms. Application development staff must not have the ability to move any software directly into the production processing environment. Controls must be in place to prevent the migration of unauthorized application code into the production environment. System privileges allowing the modification of production business information must be restricted to production applications. Privileges must be established such that system users are not able to modify production data in an unrestricted manner. Users may only modify production data in predefined ways that preserve or enhance its integrity. Updates to production databases must only be made through established channels which have been approved by the Senior Management. The use of direct database access utilities in the production environment is not permitted because these programs will circumvent database synchronization and replication routines, input error checking routines, and other important control measures.

Logs and Other Security Tools: Computer and communications systems handling sensitive or critical information must securely log all significant security relevant events. Examples of security relevant events include: Users switching user-IDs during an online session, attempts to guess passwords, attempts to use privileges that have not been authorized, modification of production application software, modifications to system software, changes to User privileges, and changes to logging subsystems.
Information Technologies Supervisor will prepare regular reports for management regarding security access issues, incidents, status, degree of compliance, changes and initiatives and other relevant events.
Reporting Problems-Reportable Incidents: Any security incident including unauthorized access or attempts, theft or disclosure of passwords or access controls, any loss, alteration or suspected disclosure of data or nay violation of security policies, procedures and standards must be promptly reported to the Information Technologies Supervisor and closest superior officers verbally, by telephone and form annexed to Data Breach Response Plan.

4. **Physical Access Control**: Physical access across the ELOPSIS premises, where restricted due to the sensitivity of resources and data within the facilities according to staff members' security clearance, is controlled primarily via ELOPSIS issued cards using RFID technology. Fingerprint scanner systems and other biometric scanners may also be used to access the areas where confidential and research and development data are stored. ID Cards and biometric scanner systems may only be used to provide physical access to areas where access is restricted to authorized personnel, and they may not be used for tracking staff's attendance.

4.1. Lost ELOPSIS Cards must immediately be reported to the Information Technologies Supervisor which will cancel the card through the Company's physical access control system. Replacement cards cannot be issued until the Information Technologies Supervisor has confirmed that a prior card has been cancelled. New cards with the same level of access control will be issued in this case.

4.2. **Access Control System Data**: The data held by the university in relation to the Access Control System includes the following categories of data:

- Cardholder data
    - Name and Middle Name-Surname
    - Title
    - Department/Unit
    - E-Mail address
    - Staff number
    - Mobile Number
- Cards allocated to cardholders
- Locations, dates and times of card reads

4.2.1. The access control data is accessible by staff who require the access control terminal software to carry out their duties. This includes:

- Security Officers
- Staff members who issue cards and alter access rights
- IT Technical Support Staff

4.2.2. Where data is released from the access control system, in compliance with the processes set out in this Policy, where practically possible, all fields which make the data identifiable as belonging to a specific person should be removed. For example, if a request to know how many people used a reader during a certain period, the report need not include the names of the cardholders, their photographs, or any other personal information, just the quantity of card reads.

4.3.Access Control Methods

Access to data is variously and appropriately controlled according to the data classification levels described in Information Asset Register Procedure.

Access control methods used by default include:

• explicit logon to devices,
• Windows share and file permissions to files and folders,
• user account privilege limitations,
• server and workstation access rights,
•, firewall permissions,
• network zone and VLAN Access Control Lists,
• intranet/extranet authentication rights,
• ELOPSIS user login rights,
• Database access rights and ACLs,
• Encryption at rest and in working,
• Any other methods as contractually required by interested parties

4.4.Access control applies to all ELOPSIS-owned networks, servers, workstations, laptops, mobile devices and services run on behalf of the Company.

4.5.Role-based access control (RBAC) will be used as the method to secure access to all file-based resources contained within ELOPSIS's Active Directory domains.

4.6.Penetration Tests: ELOPSIS's access control provision will be regularly made subject to penetration tests, in order to ascertain the effectiveness of existing controls and expose any weaknesses. Tests will include, where appropriate and agreed to, the systems of cloud service providers.

ACCESS CONTROL DATA REQUEST PROCESS