Logical Access Policy

Version 3.0

12th February 2020

Document History

Created by:	Eddy Lareine
Approved by:	Areff Salauroo

Release date	Version	Change Details	Reviewed by
22.10.19	1.0	Submitted for review	Legal Advisor
12.11.19	2.0	Apply changes submitted by legal advisor	Eddy Lareine
12.02.20	3.0	Submitted for review	Areff Salauroo

Table of Contents

LOGICAL ACCESS POLICY

1.0 Objective

The objective of this policy is to control and limit access on a "need-to-have" basis, to information, information processing facilities and business processes within La Sentinelle Ltd in order to protect and preserve the confidentiality, integrity and availability of company's information.

2.0 Scope

This policy applies to all employees and Third Parties of La Sentinelle Ltd who have access to company's information and use IT facilities and equipment.

3.0 References

3.1 References to ISO 27001:2013

- **Access Control Policy – A.9.1.1**
  An access control policy shall be established, documented and reviewed based on business and security requirements.

- **User Registration and De-Registration – A.9.2.1**
  A formal user registration and de-registration procedure is implemented to enable assignment of access rights.

- **User Access Provisioning – A.9.2.2**
  A formal user access provisioning process shall be implemented to assign or revoke access rights for all user types to all systems and services.

- **Management of Privileged Access Rights – A.9.2.3**
  The allocation and use of privileged access rights shall be restricted and controlled.

Rue des Oursins, 21731, Baie du Tombeau I T : +(230) 206 8200 I F : +(230) 247 1010 I E : corporate@lasentinelle.mu

- **Management of Secret Authentication Information – A.9.2.4**
  The allocation of secret authentication information shall be controlled through a formal management process.

- **Review of User Access Rights – A.9.2.5**
  Asset owners shall review users' access rights at regular intervals.

- **Removal or Adjustment of Access Rights – A.9.2.6**
  The access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.

- **Information Access Restriction – A.9.4.1**
  Access to information and application system functions shall be restricted in accordance with the access control policy.

- **Secure Log-on Procedures – A.9.4.2**
  Where required by the access control policy, access to systems and applications shall be controlled by secure log-on procedures.

- **Access Control to Program Source Code – A.9.4.5**
  Access to program source code shall be restricted.

3.2 References to Policies and Forms

- Asset Policy
- Password Policy
- Network Access Policy
- Human Resources Policy
- Change Management Policy
- Information Security Incident Management Policy
- User Registration and De-Registration Form
- Computer Services Request Form
- Network Access Request Form

4.0 Policy Description

4.1 Access to Secret, Confidential and Internal Use Information

Access to 'Secret', 'Confidential', and 'Internal Use' information shall be limited to authorised persons whose job or responsibilities require it, as determined by law, contractual agreement with concerned stakeholders or the Information Security Policy. Access to any of these resources shall be restricted by use of firewalls, network segregation, secure log-on procedures, access control list restrictions and other controls as applicable.

The responsibility to implement access restrictions lies with the data processors and data controllers, but must be implemented in line with this policy.

Role-based access control shall be used as the method to secure access to all file-based resources contained within La Sentinelle Ltd Active Directory domains and administered by La Sentinelle Ltd IT Department and/or sub-contractors.

There shall be no restrictions on the access to 'Public' information.

4.2 Access Control

Access control applies to all La Sentinelle Ltd owned networks, servers, workstations, laptops, mobile devices and services run on behalf of La Sentinelle Ltd.

La Sentinelle Ltd will provide all employees, suppliers 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. The Logical Access Control Policy shall be established, documented and periodically reviewed, based on business needs and external requirements. The business requirements for access control shall be based on the following principles:

- Access to information must be specifically authorized in accordance with La Sentinelle Ltd User Access Control procedures.

- Access to information will be controlled on the basis of business and security requirements, and access control rules defined for each information system.

- All users must be allowed access only to those critical business information assets and processes, which are required for performing their job functions.

- Access to critical business information assets and activation of user accounts for contractors, consultants, temporary workers, or vendor personnel must only be in effect when the individual is actively performing service for La Sentinelle Ltd.

- For Contractors, Consultants, Vendor Personnel or other Third Parties, access to La Sentinelle Ltd critical business information assets, will be provided only on the basis of a contractual agreement.

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 ACLs (Access Control Lists)
- IIS(Internet Information Services)/Apache intranet/extranet authentication rights,
- La Sentinelle Ltd user login rights,
- Database access rights and ACLs (Access Control Lists),

The Access Control policies shall include:

- Clearly stated rules and rights based on user profiles. Role-based access control shall be used as the method to secure access to all file-based resources contained within La Sentinelle Ltd Active Directory domains.

- Consistent management of access rights across a distributed/networked environment.

- An appropriate mix of logical (technical) and physical access controls.

- Segregation of access control roles e.g. access request, access authorization, access administration

- Access on a 'Need-To-Know' or 'Need-to-Have' principle i.e. access shall be granted at the minimum level necessary for the role. Users can get read or write privileges depending on their specific roles and functions.

- Requirements for formal authorisation of access requests.
- Requirements for authorisation and timely removal of access rights when an employee is terminated.
- Implement mechanisms to prevent unauthorized access to server file systems such as restrict direct-write access or installing software or even accessing other user's files.

4.3 User Registration and De-Registration

A formal User Registration and De-Registration procedure shall be put in place for granting and revoking access to all information systems and services as follows:

- A formal record of every individual registered to gain access to the required facilities and services shall be maintained in the form of a ***User Registration/De-registration Form*** or ***Computer Services Request form*** *or* ***Network Access Request Form*** *as* applicable. The User Registration/De-Registration Form will consist of a written statement of each user's rights and responsibilities
- The ***User Registration/De-Registration Form*** or ***Computer Services Request form*** *or* ***Network Access Request Form*** must be duely completed, approved and signed by an authorised Head of Department or Manager of the user. The Head of Department or Manager of the user shall ensure that the user's access rights are consistent with the business purpose and the Logical Access Policy.
- A copy of the User Registration/De-registration form shall be given to the user for reference while another copy shall be kept in a Folder by the System Administrator.
- Access to IT resources and services shall be given through the provision of a unique user account and complex password.
- Each user shall be assigned a unique User ID and Password.
- Temporary users (e.g. Consultants, Suppliers, Sub-Contractors or Third Parties) shall also need to fill a ***User Registration Form*** or ***Computer Services Request Form*** *or* ***Network Access Request Form*** for necessary access.
- Access shall be granted after completion of all authorisation procedures and acceptance/approval of Head of Department / Manager.

- On termination of an employee or expiry of temporary user access, access rights to all respective services and applications shall be removed immediately. The User Registration/De-registration Form shall consist of a section which will require the approval and signature of the leaving user's Head of Department/Manager/Team Leader in order to proceed with the de-activation of the user's access to the required services and applications immediately after the departure of the employee or on notification of termination, as applicable.

- Any change in access rights shall be documented by filling in a new ***User Registration Form*** or ***Computer Services Request Form*** *or* ***Network Access Request Form***.

- Users' access rights shall be reviewed at regular intervals and after any changes, such as promotion, demotion, or termination of employment.

4.4 Privilege Management

La Sentinelle Ltd shall employ the concept of least privilege, allowing only authorized accesses for users which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.

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. Authorisation for the use of such accounts will only be provided explicitly, upon written request from a Senior Management team member, e.g. Head of Department, General Manager or Senior Manager, and will be documented by the system administrator.

The allocation and use of privileges shall be restricted and controlled as follows:

- All Access privileges (such as System Administrator) associated with each system/application and the users to which they need to be allocated shall be identified.

- Technical teams will be required to guard against issuing privilege rights to entire teams to prevent potential losses of confidentiality and / or integrity.

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

- Privileges shall be allocated to users on a "Need-To-Use" basis and on an "Event-By-Event" basis.

- Privileges shall be documented and authorized by filling in a User Registration/De-Registration Form, Computer Services Request Form or Network Access Form, as applicable.
- Privileges granted to temporary users shall be removed promptly after the intervention of such users.
- Privilege allocations shall be checked at regular intervals to ensure that unauthorized privileges have not been obtained. In case unauthorized privileges are found, a security incident is raised and dealt with as per **Information Security Incident Management Policy**.
- Changes to privileged accounts are logged for periodic review.

4.5 Review of User Access Rights

La Sentinelle Ltd shall establish a process to review users' access rights as follows:

- User access rights shall be reviewed every 6 months, and after any changes, such as, promotion, demotion, or termination of employment.
- User access rights shall be reviewed and re-allocated when moving from one employment to another within the same organisation.
- Authorisations for privileged access rights shall be reviewed every 3 months.
- Privilege allocations shall be checked every 3 months to ensure that unauthorised privileges have not been obtained;
- Changes to privileged accounts shall be logged for periodic review.

4.6 Information Access Restriction

Access to information and application system functions by users and support personnel shall be restricted in accordance with defined access control policy. Restrictions to access shall be based on individual application requirements.

- The System Administrator shall grant access rights based on requests from authorised Head of Departments / Managers, to staff by defining who will have access to an application, level of access and functionalities, including read, write, delete and/or execution access.
- On termination of an employee and notification to Head of IT Department, the System Administrator shall ensure the removal of access rights of that employee.
- System Administrator must provide access menus on user screens that control access to application systems and their functions through a Login and secret password for authentication.
- Provision of access rights shall be limited so that even if users bypass system menus, they cannot access unauthorised applications or system functionalities.

4.7 Sensitive System Isolation

All sensitive systems must have an isolated and highly secured computing architecture. The sensitivity of an application system must be explicitly identified and documented by the system administrator. Special handling of sensitive application systems shall require that:

- They run on a dedicated and secured server.
- Resources are shared only with trusted applications systems after corresponding risks are identified, assessed and accepted by the owner.
- Isolation is achieved using physical and logical methods and the sensitive application system may be subject to dis-connection from the corporate network depending on the outcome of the Business Impact Analysis.

4.8 Access Control to Program Source Code

Access to program source code and associated items such as system designs, functional specifications, technical specifications, verification plans and validation plans, shall be strictly controlled, in order to prevent the introduction of unauthorized functionality and to avoid unintentional changes. This shall be achieved by central storage of such code in program source libraries. Access to these program source libraries is controlled and following measures are taken:

- Program source libraries shall not be stored in operational systems.
- Procedures shall be established to manage program source codes, versioning and libraries.
- Support personnel shall not have unrestricted access to source libraries.
- Updating of source libraries and associated items, and the issuing of source codes to programmers shall be only performed following authorisation from authorized personnel.
- Program listings shall be held in a secure environment, such as safes and access is limited to authorized personnel only.
- An audit log of all accesses to program source libraries shall be maintained.
- Maintenance and copying of program source libraries shall be done in line with the ***Change Management Policy.***

4.9 Cloud Systems

The use of cloud-based systems by La Sentinelle Ltd must in all respects meet the access control provisions laid out in this policy. Evaluation of access controls implemented in any cloud system shall be performed during the vendor assessment and implementation stages of any project through a Business Impact Analysis and Risk Assessment. If risks will be deemed too high, the project will need to be approved by the **Board or Risk Committee** prior to committing the system to the cloud.

5.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action that may lead to and including termination of employment. A violation of this policy by a temporary worker, contractor, vendor or third party may result in the termination of their contract or assignment with La Sentinelle Ltd.

6.0 Logical Access Policy Agreement

I have read and I understand the Logical Access Policy and its related contents. I understand that I must comply with the instructions and guidelines given therein and if I violate the rules explained herein, I may face legal or disciplinary action according to applicable laws or company policy.

Name : _____

Signature : _____

Date : _____