SILVERSEA
*Above and Beyond All Expectations℠*

# Access Control Policy
## Information Security System

| | |
|---|---|
| **Valid From** | **xx.xx.2021** |
| **Responsible** | CIO |
| **Publication** | SilverHR |
| **Version N°.** | 0.1 |
| **Last Review** | xx.xx.2021 |

# Table of contents

# 1 Aim and purpose

In order to strengthen the security and confidentiality of information, the Company has established specific requirements for protecting information and information systems against unauthorized access.

Information security is the protection of information against accidental or malicious disclosure, modification or destruction. Information is an important, valuable asset of the Company which must be managed with care.

All information has a value to the Company. However, not all of this information has an equal value or requires the same level of protection.

Access controls are put in place to protect information by controlling who has the rights to use different information resources and by guarding against unauthorized use.

The purpose of this policy is to ensure that the Company has adequate controls to restrict access to data and systems to only authorized users or processes. Access control rules and procedures are required to regulate who can access Company information resources or systems and the associated access privileges. This policy applies at all times and should be adhered to whenever accessing the Company's information in any format, and on any device.

# 2 Scope

This Company directive is valid for all bodies and employees of Silversea and its affiliates. This policy applies to all users: partners, company employees, contractual third parties and agents who use company provided ICT facilities and equipment, or have access to, or custody of, company information. More specifically:

- **Employees**: they exist in the HR system with a full set of data.
- **Temporaries (individual)**: if they hold an HR contract, they have the same information of employees plus a termination date (contract end date)
- **Contractor (company)**: an external supplier may use different of its employees to provide services that requires IT resources to Silversea. In this case each individual is recorded as a contractor.
  - Each contractor should belong to a company. Each contractor has an expiration date that eventually coincides with the contract end date of his company
  - Company: they must have a contract with an expiration date; a company may have several contracts
- **Seaman**: holds a contract with an expiration date.

All users must understand and adopt/use this policy and are responsible for ensuring the safety and security of the Company's systems, information and data that they use.

All users have a role to play and a contribution to make to the safe and secure use of technology and the information/data that it holds.

# 3 Definitions

- ***Access Control*** is the process that limits and controls access to resources of a computer system.
- ***Users*** are employees, consultants, contractors, agents and authorized users accessing Silversea IT systems and applications.
- ***System or Application Accounts*** are user ID's created on IT systems or applications, which are associated with specific access privileges on such systems and applications.
- ***Privileged Accounts*** are system or application accounts that have advanced permissions (as compared to regular user accounts) on such systems or applications. Examples of user accounts with privileges include: administrative and super user accounts.
- ***Access Privileges*** are systems permissions associated with an account, including permissions to access or change data, to process transactions, create or change settings, etc.

- ***Administrator Account*** is a user account with privileges that have advanced permissions on an IT system that are necessary for the administration of this system. For example, an administrator account can create new users, change account permissions, modify security settings such as password settings, modify system logs, etc.
- ***Application and Service Accounts*** are user accounts that are not associated with a person but an IT system, an application (or a specific part of an application) or a network service.
- ***Nominative User Accounts*** are user accounts that are named after a person.
- ***Generic or Shared Role Account*** is a generic user ID assigned for one specific role that can be used by more than one person (e.g. Captain, Cruise Director, etc.).
- ***Non-disclosure Agreement*** is a contract between a person or a company and Silversea stating that the person/company will protect confidential information (as defined in the Record Management Policy) covered by the contract, when this person/company has been exposed to such information.
- ***CIO*** (Chief Information Officer) oversees the people, processes and technologies within a company's IT organization to ensure they deliver outcomes that support the goals of the business.
- ***CISO*** (Chief Information Security Officer) is the executive responsible for an organization's information and data security.

# 4 Guiding principles

## *4.1 General requirements*

The Company will provide access privileges to Company technology (including networks, systems, applications, computers and mobile devices) based on the following principles:

- **Need to know** – users or resources will be granted access only to systems that are necessary to fulfill their roles and responsibilities.
- **Least privilege** – users or resources will be provided with the minimum privileges necessary to fulfill their roles and responsibilities.

The user manager needs to fill a dedicated form to request or change a user account and access privileges, included special accounts and privileges (such as vendor accounts, application and service accounts, system administration accounts, shared / generic accounts, test accounts and remote access) must be formally documented in the HR system and approved by the Application Owner. The IT Department is in charge to create the user accounts and assign the related privileges in the system.

Application and service accounts must only be used by application components requiring authentication; access to the passwords must be restricted to authorized IT administrators or application developers only (for the minimum necessary time).

Where possible, the Company will set user accounts to automatically expire at a pre-set date. More specifically:

- When temporary access is required, such access will be removed immediately after the user has completed the task for which the access was granted.
- User accounts assigned to contractors will be set to expire according to the contract's expiry date (expiration date after 1 year).
- User accounts will be disabled after 3 months of inactivity.

Access rights will be disabled or removed when the user is terminated or ceases to have a legitimate reason to access Silversea systems.

Existing user accounts and access rights will be reviewed quarterly to detect dormant accounts and accounts with excessive privileges. Examples of accounts with excessive privileges include:

- An active account assigned to external contractors, vendors or employees that no longer work for the Company.
- An active account with access rights for which the user's role and responsibilities do not require access. For example, users that do not have authority or responsibility to approve expenses should not have access with approval permissions within a financial system.

- System administrative rights or permissions (including permissions to change the security settings or performance settings of a system) granted to a user who is not an administrator.
- Unknown active accounts.

All access requests and approval workflows for system/application accounts and permissions as well as for IT equipment will be managed and documented using the ***SilverHR*** portal.

## 4.2 Privileged Accounts

Where possible a nominative and individual privileged user account must be created for administrator accounts, instead of generic administrator account names.

Privileged user accounts can only be requested by Head of Departments and must be appropriately approved.

## 4.3 Shared and Functional User Accounts

Shared user accounts are only to be used on an exception basis with the appropriate approval. This includes general user accounts such as "guest" and "functional/role" accounts, especially on board, such for example "Captain" or "Hotel Director".

On board normally functional accounts are used instead of personal accounts due to the rotation of personnel (e.g. SPCaptain@silversea.com or SMChiefEngineer@silversea.com). Each account is associated to a specific person for a specific period of time (usually a few months) but to know who used the account the crew journal should be updated regularly. Exceptions may apply and must be tracked (overlapping periods when 2 people are on board with the same functional role).

Other accounts (both shore and shipside) are generic and indicate a group of people (e.g. Reception@silversea.com or invoices@silversea.com). In this case the responsibility of the user is shared among the members of the teams and these logins should not have high privileges.

In case a shared login has high privileges (e.g. administrator) the usage of the login by each owner should be tracked in a specific journal.

When shared accounts and functional accounts are required:

- Passwords will be stored and handled in accordance with the Password Policy (see chapter 5).
- When shared user accounts are reassigned:
  - A dedicated form must be filled to formally trace the handover.
  - The IT department must force the password change.

## 4.4 Vendor or Default User Accounts

All default user accounts will be disabled or changed. These accounts include "guest", "temp", "admin", "Administrator", and any other commonly known or used default accounts, as well as related default passwords used by vendors on "commercial off the shelf" systems and applications.

## 4.5 Test Accounts

Test accounts can only be created if they are justified by the relevant business area or project team and approved by the application owner, through a formal request to the CIO through the IT Service Desk.

Test accounts must have an expiry date (maximum of 1 month). Maintaining test accounts beyond this date must be re-evaluated every 90 days and approved appropriately.

Test accounts must be disabled / deleted when they are no longer necessary.

## 4.6 Contractors and Vendors

In accordance with the Contract Management Policy, contracts with contractors / vendors will include specific requirements for the protection of data. In addition, contractor / vendor representatives will be required to sign a Non-disclosure Agreement (“NDA”) prior to obtaining approval to access Silversea systems and applications.

Prior to granting access rights to a contractor / vendor, the Service Desk must verify the requirements of Section above have been complied with.

The name of the contractor / vendor representative must be communicated to the IT Service Desk at least 2 business days before the person needs access.

The IT department will maintain a current list of external contractors or vendors having access to Silversea systems by means of the application *SilverseaHR* .

The need to terminate the access privileges of the contractor / vendor must be communicated to the IT Service Desk at least 2 business days before the contractor / vendor representative’s need for such access ends.

## 4.7 Access Control Requirements

All users must use a unique ID to access Silversea systems and applications. Passwords must be set in accordance with the Password Policy.

Alternative, authentication mechanisms that do not rely on a unique ID and password must be formally approved by the CISO (if appointed) or the CIO.

System and application sessions must automatically lock after 15 minutes of inactivity.

## 4.8 Segregation of Duties

SoD (*segregation of duties*) has two primary objectives. The first is the prevention of conflict of interest (real or apparent), wrongful acts, fraud, abuse and errors. The second is the detection of control failures that include security breaches, information theft and circumvention of security controls. Correct SoD is designed to ensure that individuals do not have conflicting responsibilities or are not responsible for reporting on themselves or their superior.

SoD is critical to effective internal control; it reduces the risk of both erroneous and fraudulent actions. In general, the approval function, the accounting/reconciling function, procurement duties and the custody of assets should be separated among employees. When these functions cannot be separated, a detailed supervisory review of related activities is required as a compensating control activity.

# 5 Password Policy

Password must comply with security rules on each system:

- The minimum length must be 8 characters
- Password age must be set no longer than 90 days
- password must meet complexity criteria being:
  - at least 1 number is required;
  - at least 1 upper case letter is required;
  - at least 1 special character is required;
- The password must be different from the last 4 passwords used
- The password chose by the user must not be displayed or communicated to the user by the system.
- After 5 unsuccessful log-in attempts, the user must be temporarily blocked

Furthermore, it is required to:

- Change default passwords at the first log-in by following the above Password Policy guidelines.

In case of handover, ensure that the joining member change the password of the shared user account assigned at the first log-in.

# 6 SilverHR

SilverHR is an internal tool developed to handle the internal and external Silversea's workforce. All the users (permanent employees, temporaries, contractors, etc.) must be registered and configured in SilverHR according to their contract type. They are placed in the organization chart according to their role and appended under their manager. The "Onboarding" procedure allows the manager to request the IT equipment and System access that they need to accomplish their tasks.

SilverHR manages the approval workflows and the equipment/access dismissal/removal at the end of the contractual period or when an employee leaves the Company.

# 7 Roles and Responsibilities

The CISO if appointed otherwise the CIO has ultimate responsibility for compliance of this policy.

The ICT Department is responsible for detailing and reviewing the procedures.

Heads of Departments are responsible for ensuring that themselves and their staff adhere to this policy and receive training to help maintain security and confidentiality of information.
All employees, contractors and third party users are required to adhere to the policies principles and procedures.

HR Department, the user manager and the System Owners are responsible for an effective application of the policy in respect of the "least privilege" principle.

The CIO is ultimately responsible for:

- Monitoring the ICT infrastructure.
- Dealing with user access controls.
- Reporting and providing advice to the Executive Board in respect of disciplinary matters where it is suspected that the Company's Policies have been breached.
- Maintaining and reviewing the procedure in respect of Information Security Management policy.

The VP Audit advises the System Owners in the definition and enforcement of the minimum Segregation of Duties rules.

# 8 Policy Compliance

All users are personally responsible for adhering to all specifications in the area of information security. They are obliged to gain the necessary information on the applicable security specifications and to report incidents, dangers and security flaws to their Head of Department.

If you do not understand the implications of this policy or how it may apply to you, seek advice from the IT Support.

It will be a breach of this policy for any user to misuse their authentication credentials. If any such misuse results in a user knowingly elevating their system privileges, above those that they have been authorized to use, this will be considered an act of gross misconduct.

Violations of this directive can result in disciplinary action and/or civil prosecution.

# 9 ANNEX – Application Owner

| Software & Utilities | Owner |
|---|---|
| Silversea Windows Domain Account | CIO |
| Silversea Email Account | CIO |
| MS Office Standard | CIO |
| Citrix | CIO |
| VPN | CIO |

| System / Application | Owner |
|---|---|
| Amos | SVP Technical Operations |
| PMS Fidelio | Director Newbuild & Revite |
| File server (documents) | CIO |
| My Cruise (information entertainment system) | Director Newbuild & Revite |
| Silver Compass | Director Newbuild & Revite |
| Restaurant Reservation | Director Newbuild & Revite |
| Table Assignment | Director Newbuild & Revite |
| Remote Ordering | Director Newbuild & Revite |
| Menu Management/Printing | Director Newbuild & Revite |
| POS | CFO |
| Online Comment Card | Director Newbuild & Revite |
| On Boarding Platform | Director Newbuild & Revite |
| Bunker Web | SVP Technical Operations |
| MXP | Senior Director Port Operations |
| Calc Menu - Kiosk | Director Newbuild & Revite |
| Pressreader | Director Newbuild & Revite |