# Access Control Policy

## O’Brien Landscaping

**Developed by**

**Barry Lupton**

**Version 1.0**

## Document Control

Author(s): O'Brien Landscaping

Owner: Barry Lupton

Distribution: Directors

| Pages | Version Number | Date |
|---|---|---|
| | 1.0 | 4th May 2019 |

# Corporate Access Control Policy

**Purpose**

The purpose of this policy is to preserve the confidentiality, integrity and availability of O'Brien Landscaping 's' information. Controls outlined in this document are implemented to ensure that people have the right access to the right information at the right time.

**Objectives**

The implementation of this policy is to control access to information to both physical and logical which is cover by this policy.

The procedures covered in this policy cover all stages in the life-cycle of user access, from the initial registration of new users to the final de-registration of users who no longer require access to information systems and services.

The policy is structured under the following headings:

- User access management
- User responsibilities
- Network access control
- Operating system access control
- Application and information access control
- Mobile computing and teleworking

**User Access Management**

Objective: To ensure authorized user access and to prevent unauthorized access to information systems.

*User Registration*

There is a formal user registration and de-registration procedure in place for granting and revoking access to all information systems and services

- On commencement of employment the following will occur:
    - The Directors decide on the appropriate access rights and privileges and complete the New User Access Rights Document.
    - A support ticket will be created to create the required accounts with relevant suppliers.
- There will be immediate removal of access rights of users who leave the organization. The directors shall ensure that the users rights are revoked by creating a support ticket(s).
- The management will be responsible for maintaining a formal record of all persons registered to use the systems and for ensuring that redundant user IDs are not issued to other users.
- If an employee's role changes within the organisation the directors will review the required access rights and make changes where required following the above procedure.

*Privilege Management (The rights to install or modify the operating system or software on a device)*

O'Brien Landscaping does not permit any privileges to any staff members to edit code within any operating or business application without the approval of the DOT.

*User Password Management*

Allocations of passwords are controlled through a formal management process.

- A confidentiality clause is included in the employee handbook, which forms part of the employment contract.
- Users are provided with a user ID and a temporary complex password upon commencement of employment. Users are forced to change the temporary password immediately and should acknowledge receipt of it.
- Passwords should never be stored on computer systems in an unprotected form.

*Review of User Access Rights*

- Management will review users' access rights if/when there have been any changes such as promotion, demotion or termination of employment.
- A support ticket will be raised to request the change
- These changes will be recorded in the minutes of the quarterly health checks.

**User Responsibilities**

Objective: To prevent unauthorized user access, and compromise or theft of information and information processing facilities.

*Password Use*

Users are required to follow good security practices in the selection and use of passwords.

- Users must use complex passwords; this is forced by the server policies.
- Keep passwords confidential.
- A record of the password should not be kept (e.g. paper, hand-held device or software file) unless it can be stored securely and the method of storing has been approved by management.
- Passwords are not included in any automated log-on process.
- Entry to system passwords are to be changed on every 90 days.
- Business application passwords should be changed upon request from the Director of Finance & Security (DOFS) as determined by business or security needs.

*Unattended User Equipment*

Management ensure that unattended equipment has appropriate protection.

- All PCs/laptops are password protected using screen savers.
- Users must log-off servers and office PC's when the session is finished.

*Clear Desk Policy*

Employees should adhere to the clear desk policy for papers and removable storage media.

- Physical paperwork should be locked away when leaving the office.
- Documents containing sensitive or classified information should be removed from printers/photocopier immediately.

**Network Access Control**

Objective: To prevent unauthorized access to network services

*Policy on use of network services*

Users are only provided with access to the services that they have been specifically authorized to use. In line with the conditions set out in the above "User Access Management" outlined in the 'Access Rights Document':

- On commencement of employment users will be provided with:
  - An email statement of their access rights.
  - A unique user ID.
- Management have the following controls and procedures in place to protect access to network connections and services:
  - Sufficient network perimeter security
  - Use of complex passwords.
- Access to network resources such as remote desktop, file access and non-web enabled applications can only be access using a secure VPN connection. The VPN user ID is not associated with the user's active directory account.
- Access to web enabled applications such as Outlook Web Access manager is permitted and controlled by the active directory security policy.
- External vulnerability scans are run on an annual basis.

*User Authentication for External Connections in use*

Appropriate authentication methods are used to control access by remote users by:

- Access to network resources such as remote desktop, file access and non-web enabled applications can only be access using a secure VPN connection. The VPN user ID is not associated with the users' active directory account.

*Equipment Identification in Networks*

Each device attached to the O'Brien Landscaping internal network must be approved by the DOT/SM. Physical access to the Server Cabinet/server room is required in order to add any new equipment to the network.

*Remote Diagnostic and Configuration Port Protection*

There is no access to ports remotely.

*Segregation in Networks*

The nature of O'Brien Landscaping 's business does not require segregation of the network.

There are two networks O'Brien Landscaping with appropriate firewalls in place:

1. Peter O'Brien Landscaping, Swords Enterprise Park
2. Peter O'Brien Landscaping, Streamstown

*Network Connection Control*

User's access to the network is restricted by:

- Physical access to the Server. The server is located in locked building.
- Access to network resources such as remote desktop, file access and non-web enabled applications can only be access using a secure VPN connection. The VPN user ID is not associated with the user's active directory account.
- Data and passwords are transmitted using a trusted SSL certificate.

*Network Routing Control*

Physical access is by means of a secure code locked building.

**Operating System Access Control**

Objective: To prevent unauthorized access to operating systems.

*Secure Log-On Procedures*

Access to operating systems is controlled by the following secure log-on procedure:

- Accounts will be locked out following five unsuccessful log-on attempts
- The password is never displayed; it is hidden by symbols.
- User connection time is limited to screen saver at 15-minute inactivity

*User Identification and Authentication*

All users in O'Brien Landscaping  are given a unique identifier (user ID) upon commencement of employment and are required to use passwords. User ID's are used to trace activities to the responsible individual.  User ID's are created in an Active Directory tree at level 2016.

*Password Management System*

Passwords are selected and maintained by users after the initial temporary password have been provided by O'Brien Landscaping or third-party support. The system for managing passwords is interactive and ensures quality passwords by:

- Users have to change the temporary password at the first log-on.
- Users are allowed to select and change their own passwords.
- Passwords must be complex in structure.
- Enforcement of password changes occurs every 90 days.
- Passwords are not displayed on the screen when they are entered.

*Use of System Utilities*

Installation of third party applications or utilities must be approved by the DOT.

The use of file sharing or peer to peer sites is forbidden within the O'Brien Landscaping network.

Screen savers are enabled on all O'Brien Landscaping equipment, the time out is set by group policy at 15 minutes. There are no limitations on connection times.

**Application and Information Access Control**

Objective: To prevent unauthorized access to information held in application systems.

*Information Access Restriction*

Access to information and application system functions by users are restricted in accordance with the access rights record.

*Sensitive System Isolation*

Applications/cloud services that contain sensitive data are listed in the application identification appendix.

**Mobile Computing and Teleworking**

Objective: To ensure information security when using mobile computing and teleworking facilities.

*Mobile Computing and Communications*

O'Brien Landscaping 's mobile computing policy is as follows:

- All mobile phones are password protected and encrypted
- If a mobile phone is lost or stolen, then the non-volatile memory will be remotely wiped clean by the DOT or support manager
- If the laptop is lost or stolen, then the user's active directory and VPN passwords will be changed by opening a ticket on Support Management System
- Mobile phones or laptops must not be left unattended in public places.
- Mobile phones or laptops where possible should be physically locked away to secure the equipment, and not left in company vans or private cars overnight.

*Teleworking*

O'Brien Landscaping  permit teleworking as long as the following security procedures are followed:

- Access to network resources such as remote desktop, file access and non-web enabled applications can only be access using a secure VPN connection.  The VPN user ID is not associated with the user's active directory account.
- Access to web enabled applications such as Outlook Web Access is permitted and controlled by the active directory security policy.
- The employee can only use their own PC/laptop with the approval of the DOT and it adheres to the security requirements for O'Brien Landscaping  computer equipment, e.g. encryption and password protection.

Signed:

Date:

ISMS Policy Owner: **CEO**