**Contents**

[1. Introduction 3](#_Toc105498925)

[2. Purpose 3](#_Toc105498926)

[3. Roles and Responsibilities 3](#_Toc105498927)

[3.1 Access Manager 3](#_Toc105498928)

[3.2 1st Level Support 4](#_Toc105498929)

[4. Access Request Form 4](#_Toc105498930)

[5. Access Management Process 4](#_Toc105498931)

[6. Assigning workplace catalog rules to user accounts 5](#_Toc105498932)

[7. Policy 6](#_Toc105498933)

[7.1 Access control 6](#_Toc105498934)

[7.2 Account Management 6](#_Toc105498935)

[7.3 Administrator/Special access 7](#_Toc105498936)

[7.4 Authentication 7](#_Toc105498937)

**Document Control**

**Document Version History**

This table shows a record of significant changes to the document.

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Author** | **Description of Change** |
| 0.1 | 27/01/2022 | Swapnil Wale | DRAFT |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Approvals**

This table shows the approvals on this document for circulation, use and withdrawal

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version** | **Date** | **Approver** | **Title/Authority** | **Approval Remarks** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

# Introduction

ITIL access management refers to the process of allowing only authorized users to access certain assets and IT services while preventing unauthorized users from doing so.

# Purpose

The primary goal of ITIL access control is to prevent unauthorized individuals from accessing data. This is highly important for a firm since key data slipping into the wrong hands could result in catastrophic damage.

# Roles and Responsibilities

## Access Manager

* The Access Manager allows authorized users to use a service while preventing non-authorized users from doing so.
* The Access Manager is responsible for carrying out the policies set forth in Information Security Management.

## 1st Level Support

1st Level Support is responsible for registering and classifying received Incidents, as well as making an immediate effort to restore a failing IT service as rapidly as possible. If no ad-hoc solution can be found, 1st Level Support will escalate the incident to a technical support group of experts (2nd Level Support). 1st Level Support also handles Service Requests and updates users on the status of their Incidents at predetermined intervals.

# Access Request Form

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Access ID** |  | **Created by:** | | Mark |
| **Access Requester:** |  | **Access Method** | |  |
| **Access Provider:** |  | **Date Requested:** | |  |
| **Subject:** | Access to Internal Antivirus systems | | | |
| **Description:** | I wish to have access to personal data base of customers to integrate with the analytics tool | | | |
| **Approver:** |  | | **Signature:** |  |

# Access Management Process

* Requesting Access- Requests can come in the form of a service request (in service operation) or a change request from the service desk (in service transition). Going from not having access to having access, or from one level of access to another, is an example of access. Processes for responding to inquiries should ideally be included in the service catalogue. This activity should specify who is authorized to seek access, what information is necessary, and how the request will be processed.
* Verification- This activity confirms that the person requesting access is qualified to do so. The user must establish their identification and that the request is for a legitimate business cause. Depending on the level of access, multiple levels of verification may be required. Access to read and alter financial reports, for example, should have quite different approval requirements than the verification necessary when creating a new user with default capabilities.
* Monitoring Identify Status- It's now time to grant access to the person who has been validated. If necessary, this entails adding the user to a new group. Each system that a user asks access to may need the creation of credentials. Access management's job is to make sure that the access granted does not conflict with any other access permissions that have previously been granted. Creating a catalogue of user roles and access profiles makes it easier to keep track of the various groups.
* Logging and tracing access- Your business ensures that the access granted is only used as intended by logging and tracking access changes. Keeping track of changes also protects the company from security flaws and threats. Unauthorized access, strange application activity, and a high number of incorrect login attempts should all be investigated for possible security breaches.
* Removing or restricting rights- This action entails deleting or restricting access based on user roles after it has been given. This happens when users move jobs and work in different departments or on different systems throughout their careers. Whether a user is terminated, dies, changes responsibilities, departments, or geographical locations, a mechanism for granting them the access their role requires should be in place. A good information security policy is built on the foundation of these actions. Each activity should have its own set of processes that apply to each user role.

# Assigning workplace catalog rules to user accounts

To access the Workplace Catalog dashboard, you'll need a user account with an administrator, supplier, or manager role. A user account with the agent role can see the Service Requests report by logging into Digital Workplace Catalog. Only one of the following roles can be assigned to a user:

|  |  |
| --- | --- |
| **User role** | **Description** |
| Administrator | All parts of the service catalogue, including templates, service level agreement (SLA) policies, cost changes, and fulfilment procedures, are maintained by the administrator, also known as catalogue administrator. |
| Internal Supplier | An assigned sub catalog is maintained by the internal supplier. Without the application administration capabilities, the internal supplier has the same service management capabilities as the catalogue administrator. Internal service suppliers must submit services for approval before they may be made available to end customers. |
| Internal Supplier administrator | An assigned sub catalog is maintained by the internal supplier administrator. Without the ability to administer applications, the internal supplier administrator has the same service management skills as the catalogue administrator. Services are approved and published by internal service supplier administrators. |
| Agent | Service agents look into the status of service requests and respond to user questions regarding their requests. |

# Policy

## Access control

* Prior to approval, access to (District/Organization) Information Resources must be justified by a legitimate business need.
* User identification must be verified in person before access is given when multifactor authentication is used.
* Ownership responsibilities for (District/Organization) Information Resources must be established and documented.
* When such data is not backed up, disaster recovery plans must include documented user access rights and privileges to Information Resources.

## Account Management

* Access to confidential data must be recorded.
* All accounts must be uniquely identifiable using the user name provided by (District/Organization) IT, and there must be no duplicate user IDs.
* Following the principle of "least privilege," only the level of access required to accomplish allowed tasks may be granted.
* Access to Information Resources should be offered to user groups rather than individual accounts whenever possible.

## Administrator/Special access

* Account management guidelines, paperwork, and authorization are required for administrative/special access accounts.
* Personnel with Administrative/Special access accounts must not misuse their positions of power and must only carry out the tasks necessary to complete their job functions.
* Personnel having Administrative/Special access accounts must use the account privilege that best suits the task at hand (i.e., user account vs. administrator account).
* When an individual with access to a shared Administrative/Special access account changes roles, moves to another department, or quits the (District/Organization), the password for that account must be changed.

## Authentication

* Personnel are obligated to keep personal authentication information secret.
* Any group/shared authentication information must only be shared among the group's authorized members.
* If issued, security tokens (such as a smartcard) must be returned on demand or when the connection with the (District/Organization) ends.
* If the security of a password is in question, it should be changed right away.
* Administrators/Special Access users shall not, for the sake of convenience, evade the (District/Organization) Authentication Standard.
* Without activating a password-protected screensaver or logging off of the device, computing devices should not be left alone.