Access Management

*Version 1.0, 01.12.2020*

**Document Approval**

The undersigned acknowledge they have reviewed the *Access Management process*. The undersigned herby give full approval to the content of the document.



|  |  |  |
| --- | --- | --- |
| **Title** | **Name** | **Signature** |
| Quality Manager | Mary Check |  |
| General Manager | High Vision |  |

This document is reviewed and approved by management through the company’s Integrated Management System Steering Committee who is responsible to officially authorize its publication. Any change requests to this document can only be submitted to the Quality & Internal Audit department for further processing.

**Document Information**

|  |  |  |  |
| --- | --- | --- | --- |
| **Document Owner:** | Information Security Manager | **Issue Date:** | 01 December 2020 |
| **Email:** | [SiAll@AlphaBetaPrinting.com](mailto:SiAll@AlphaBetaPrinting.com) | **Last Review Date:** |  |
|  |  | **Next Review Date:** |  |



**Document History**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Author** | **Date** | **Changes** |
| 0.1 | Information Security Manager | 01/09/2020 | Initial draft issued for review & comments |
| 0.2 | Information Security Manager | 01/10/2020 | Second draft issued for review & comments |
| 1.0 | Information Security Manager | 01/12/2020 | Issued for Implementation |
|  |  |  |  |

Table of Contents

[1. Introduction 3](#_Toc59961060)

[1.1 Scope 3](#_Toc59961061)

[1.2 Owner 3](#_Toc59961062)

[1.3 Information Security and Health & Safety Aspects 3](#_Toc59961063)

[2 Policy Statements 3](#_Toc59961064)

[3 Procedures & Guidelines 4](#_Toc59961065)

[3.1 Password Usage 4](#_Toc59961066)

[3.2 Physical access management 4](#_Toc59961067)

[3.3 Process of granting or revoking access rights 4](#_Toc59961068)

[4 Records 5](#_Toc59961069)

[5 Key Performance Indicators 5](#_Toc59961070)

# Introduction

The purpose of this document is to describe how access to company’s assets is controlled. The objective of this process is to control and monitor access to any valuable company asset on the basis of potential impact an access policy violation would have to the organization.

## Scope

This document is applicable to all the company’s departments, organization-wide.

## Owner

The Information Security Manager is identified as the owner of this document who is also the only authorized person to apply any changes.

## Information Security and Health & Safety Aspects

No health & safety requirements apply to this document.

With regards to information security requirements, care should be exercised for the protection of Confidentiality, Integrity and Availability of all the documents and respective records created as part of implementing the quality and information security procedures. This protection should be applied through proper access control mechanisms as described in the “Access Management” and the “Acceptable Use Policy”.

# Policy Statements

Access to company’s information, information processing facilities and business processes is controlled on the basis of business and security requirements.

Access to company’s software applications depends on the data stored to or transmitted by each application and decisions are taken on the basis of data classification.

Access to data stored in company’s information processing facilities is subject to information handling and data privacy legislation in the country as well as contractual obligations of the company.

Process owners are responsible to define the access rights to information used by each particular process.

Access to the company’s information from the outside (remote access) is permitted under specific conditions and under strictly controlled and monitored environments.

Access rights are provided using specific IT operating procedures and are based on the use of unique and strictly personal user name and password. Use of the same user name and password from two different people is strictly prohibited. Access monitoring and controlling is based on user names and machines identifications (e.g. MAC addresses, IP addresses).

Access rights are subject of review at least annually for all company’s personnel. Process owners are required to inform IT Department for any necessary change or removal of access rights due to employment change or termination.

# Procedures & Guidelines

## Password Usage

User password is strictly personal. Sharing passwords between users is strictly prohibited.

User password changes every 90 days and cannot be changed earlier than 1 day. New passwords shall be different from the previous 3 already used. System notifies users for password change 7 days before expiration.

User passwords are at least 7 characters long, cannot contain the user name, first name and last name and they are created using characters from at least 3 of the following groups: Capital Letters, Small letters, numbers and symbols.

After 5 failed logon attempts the user account remains locked for 10 minutes and it cannot be unlocked right away.

Users with administrator and/or operator privileges have their own privileged account. This account is used only for network operation and administration and not in normal user activities.

There is a dedicated service account for each network service running on each server.

## Physical access management

Access to the company’s premises is strictly controlled.

All company employees, get access to the areas required based on the function and role. Access is controlled through an electronic access control system.

Badges are issued only to employees of the company during the onboarding process. The exact process is depicted in the Physical Security Procedure.

All visitors are escorted at all times when in the company’s premises.

The access control cards are strictly personal and sharing between employees or non-employees is not allowed.

## Process of granting or revoking access rights

| **S/N** | **Role** | **Responsibility** | **Comment** |
| --- | --- | --- | --- |
| 12.1 | Requester  (Department Manager or HR manager) | Send request | The Requester sends an electronic request through the IT ticketing system of the company in order to get permissions / or revoke permissions on an information resource / asset / processing facility etc. |
| 12.2 | IT staff | Receive request | The IT staff will receive a request through the It ticketing system. |
| 12.3 | Management | Approved | The direct management will receive an approval request from IT. |
| 12.4 | IT staff | Give Permissions | The IT staff will set the required permissions to the user as requested by the requester. |
| 12.5 | IT staff | Update the system | The IT staff will update the system. |
| 12.6 | IT staff | Close request | The IT staff will inform the user regarding their username, password, privileges and basic rules and close the request. |

# Records

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **S/N** | **Record Name** | **Record Type** | **Retention Time** | **Responsible** | **Location** | **Classification** |
| 1. | IT ticketing system | Electronic (DB) | Indefinitely | IT Manager |  | Confidential |
| 2. | Logs | Electronic | 3 months | IT Manager | In the syslog server | Confidential |

# Key Performance Indicators

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **KPI Name** | **Periodicity** | **Responsible** | **Location** | **Target** |
| Percentage of incidents that involved inappropriate security access or attempts at access to services | Annual | Information Security Manager | IT Department | Less than 5% |
| Number of audits findings that discovered incorrect access settings for users that have changed roles or left the company | Annual | Information Security Manager | IT Department | 0 |
| Number of incidents caused by incorrect access settings | Annual | Information Security Officer | IT Department | 0 |