Access Control Policy

Title

Access Control Policy

Version Control

Owner	Version	Edited By	Date	Comments
Coach Direct	0.1	KL	19/07/16	First Draft

Distribution

Held By	Format	Location	Comments
	Digital / Physical		

Status

X	Status	Approved By	Date
	Working		
X	Draft		
	Provisional Approval		
	Publication		

Classification

	Please refer to ISMS 02 Information Handling & Classification Procedure
X	**Confidential**
	Restricted
	Unclassified

Relevance to Standard

Standard	Clause	Title
ISO 27001:2013	A9.1.1	Access Control Policy

Access Control Policy

1.0 Overview

This Access Control policy defines the rules, rights and restrictions applied to users for both logical and physical access to the organisation's assets.

1.1 Principles

Need-to-know: you are only granted access to the information you need to perform your tasks (different tasks/roles mean different need-to-know and hence different access profile).

Need-to-use: you are only granted access to the information processing facilities (IT equipment, applications, procedures, rooms) you need to perform your task/job/role.

2.0 Policy

2.1 Security of Systems

The organization uses several systems to operate effectively, and it's important to maintain the confidentiality, integrity and availability of these information assets through this access control policy.

Threats associated with the information assets have been considered and addressed as far as possible through the risk management process.

2.2 Security of Networks and Services

Access to the organisations networks shall be limited to prevent unauthorized and unintended consequences.

Devices will not be connected to the network without authorization from the **IT Support Company**.

The WIFI connection details will not be shared without the authorization of the **IT Support Company.**

Guests, visitors and third parties will use ONLY the visitor WIFI network made available.

2.3 Physical Security

The physical security of the organisation's assets, including buildings and offices, should be considered at all times.

Please ensure the main door is closed and secure, do not leave it ajar. All visitors and third parties must report to reception and sign in.

Challenge any strangers on-site who do not appear to be accompanied.

2.4 Access Requests

Access requests, including new user accounts, should be submitted to the IT Support Company by email.

The job functions as described by the department manager should be reviewed to ensure that the requested access is relevant and acceptable.

In the case of IT systems including Active Directory, a profile including privileges may be copied from a colleague with the same job functions.

2.5 Access Authorisation

The managing director has overall governance of access control within the company and May, for legitimate business reasons, grant or revoke access at their discretion.

Department managers are responsible for determining the access levels required by their staff and should, where possible, maintain security groups.

2.6 Access Administration

When an access request has been approved by the Gatekeeper, a record of that decision will be maintained to allow an audit trail.

The gatekeeper will provide access to the user and inform them via an appropriate method, so as to keep any username separate from a password.

Where systems allow, a temporary password will be used and the user will be required to change their password at first log-in.

2.7 Access Review

The access to systems will be reviewed on a regular basis to ensure that users are still authorized to access each system and that the privilege level assigned to that user is still acceptable.

Gatekeepers will be responsible for reviewing their own systems and may need to refer to department managers for confirmation of user requirements.

2.8 Access Removal

In cases of disciplinary or where an employee is within their probation period, access should be removed immediately.

Where a notice period has been agreed, or the user is changing job function within the company, access should be removed when it has been confirmed by their line manager.

2.9 Privileged Access

All privileged access should be reviewed against the job function before the details or assets (including access cards/fobs) are issued to the user.

The use of privileged accounts will be limited and uniquely identifiable username will be used to enable all activity under an account to the traced back to a single individual.

2.10 Logging & Monitoring

User activity is logged and may be monitored for the purposes of error detection and security.

3.0 Related Policies

Classification and Handling Policy

System Gatekeepers

The organisation uses several systems to store data, and these are administered by different people in the organisation. The table below shows the gatekeepers of those systems, who you should go to for any of the above issues.

System	Gatekeeper	Review Frequency
Active Directory	MD / IT Support	Annual
Mail Server	MD / IT Support	Annual
Sage Line 50	MD / Accounts	Annual
Iris Payroll	MD / Accounts	Annual
Intruder Alarm	MD	Annual
Website (Front)	MD / Web Dev	Annual
Website (DB)	MD / Web Dev	Annual
WIFI	MD / IT Support	Annual