BiziTel

www.bizitel.com

Access Control Policy

Bizitel provides access to information assets, systems and resources for operational purposes only.

This policy outlines the rules relating to authorising, monitoring and controlling access to Bizitel information and information systems.

1 Scope

This policy applies to any person or systems that are granted or that grant access to accounts, information or information systems owned or operated by Bizitel.

2 Objectives

Compliance with this policy enables consistent controls to be applied throughout Bizitel, minimising exposure to security breaches, whilst allowing systems and security administration and technical support staff to conduct their activities.

This policy aims to ensure that, by having the appropriate access controls in place, the right information is accessible by the right people at the right time and that access to information, in all forms, is appropriately managed and periodically audited.

3 Responsibilities

All personnel (e.g. employees, contractors, vendors and third-parties) at Bizitel must abide by relevant Information Security and Access Control policies and procedures.

All account holders must:

- Only use their account and access in accordance with the Bizitel policy
- Secure their credentials in line with the Bizitel password guidance.
- Be responsible for the systems, services and data within their control.
- Transfer services and data prior to vacating a role

All management must:

- Only sponsor access requests that have:
    - A documented request
    - Adequate and appropriate justification, based on the requester’s business need
- Document all access request sponsorships

Asset owners must:

- Periodically review access to their assets and investigate any anomalies.

Access administrators must:

- Only grant access requests that have:
    - A documented request
    - Adequate and appropriate justification, as confirmed by the sponsor
    - Documented sponsorship and subsequent approval from a relevant personnel
- Document all access granted

4 Access Control Implementation

The following headings outline the principles around how access is managed at Bizitel:

4.1 Identity Management

Formal user registration and de-registration processes are implemented to enable the assignment of identities and accounts on an individual basis.

This ensures accountability for all actions taken by employees.

4.2 Authentication Management

All account, service and platform access is managed through secure authentication controls.

4.3 Access Governance

A formal user access provisioning process is implemented to assign or revoke access rights for all user types to systems and information assets under the control of the Bizitel.

This access provisioning is based on the following principles:

Access changes for employees are primarily managed through the Starter, Mover & Leaver processes.

- All extra requests for or changes to access are documented and tracked.
- All access requests or changes require documented justification.
- Justification will be based on a simple risk assessment and the business need and will be confirmed by the request sponsor.
- All access changes granted by administrators are documented and tracked.
- Reviews of access are performed by relevant asset owners periodically.
- These principles are agnostic of account type, service, application or system.

4.4 Privileged Account Management

Privileged accounts and privileged access must be purpose driven, secure and always adhere to the principle of least privilege.

4.5 Removal or Adjustment of Access Rights

The access rights of all employees to information and information processing facilities will be removed upon termination of their employment, contract or agreement, or adjusted upon change.

Additional access to accounts, assets, systems or services are subject to review and approval on a case-by-case basis.

4.6 Access Reviews

Access to assets, services and systems will be periodically reviewed. The frequency of these reviews depends on the identified risk surrounding the asset and access in question.

It is recommended that the risk relating to each individual asset is measured and given a risk rating in line with the single asset risk assessment process, outlined in the Enterprise Risk Management policy.

Where an access review identifies an access anomaly it will be treated as a potential incident and investigated by the asset owner and information security team.

4.7 Access in Special Circumstances

There are special circumstances where extra or privileged access is needed. For all cases, access to an account, the information contained within an account or information pertaining to the activity of an account, is carefully restricted and must only be carried out with the appropriate authorisation and safeguards in place.

Appendix A below outlines the approach taken for special circumstances.

5 Supporting Information Security Policies, Procedures and Guidance

Supporting information security policies for the principles listed above can be found at bizitel.com/terms-policies

Appendix A - Access in special circumstances

Special circumstances include, but are not limited to:

Special circumstances	Detail
Information Security and System Administration	Management may access accounts and user data. Some examples of when such access may be required are; ● Business continuity. ● To detect and prevent crime (including but not limited to, fraud and unauthorised access to computer systems); ● System security protection: Virus, malware, hacking and other infected device and account prevention. ● Misuse, abuse and illegal activity investigation.

Regulatory Requests	A request for information to satisfy a regulatory request (e.g. Subject Access Request) can be made. Requests will be considered by the CTO, referring to the Data Protection Officer, Security Services and Human Resources as required.
Previous Account Owner	A request for information held against a previously active account by the account owner may be approved only after a careful review and on a case-by-case basis. Requests will be considered by the Director of IT, referring to the Data Protection Officer, Security Services and Human Resources as required.
Employee Account Access by Department	Requests must be sponsored by the CEO (or recognised designate). They will be considered by the Director of IT, referring to the Data Protection Officer, Security Services and Human Resources as required.
Law Enforcement Authorities	Requests must be directed to the Security Management Team. The relevant documentation must be completed. Requests will be considered by the Director of IT, referring to the Data Protection Officer, Security Services and Human Resources as required.
Medically Incapacitated or Deceased User Account Access	Access requests can be made to the Information Security team. Requests will be considered by the Director of IT, referring to the Data Protection Officer, Security Services and Human Resources as required.