EzCloud

Access Control Policy

1. Scope

This policy covers all EzCloud networks, IT systems, data and authorised users.

2. Policy

2.1 Principles

EzCloud will provide all customers and employees with on EzCloud services access to the information they need to carry out their responsibilities in as effective and efficient manner as possible.

2.1.1. Generic identities

Generic or group IDs shall not normally be permitted as means of access to EzCloud data, but may be granted under exceptional circumstances if sufficient other controls on access are in place.

2.1.2. Privileged accounts

The allocation of privilege rights (e.g. local administrator, domain administrator, super-user, root access) shall be restricted and controlled and not provided by default.

Authorisation for the use of such accounts shall only be provided explicitly, upon written request from a Product manager, and will be documented by the system owner.

Technical teams shall guard against issuing privilege rights to entire teams to prevent potential losses of confidentiality and / or integrity.

2.1.3. Least privilege and need to know

Access rights to both physical and logical assets will be accorded following the principles of least privilege and need to know.

2.2 Access Control Authorisation

2.2.1. User accounts

Access to EzCloud IT resources and services will be given through the provision of a unique user account, complex password and 2FA .

2.2.2. Passwords

Password issuing, strength requirements, changing and control will be managed through formal processes.

2.2.3. Access to Confidential, Restricted and Internal Use information

Access to ‘Confidential’, ‘Restricted’ and ‘Internal Use’ information will be limited to authorised persons whose job requires it, as determined by law, contractual agreement with interested parties or the Information Security Policy.

Access to any of these resources will be restricted by use of firewalls, network segregation, secure log-on procedures, access control list restrictions and other controls as appropriate.

The responsibility to implement access restrictions lies with the data processors and data controllers, but must be implemented in line with this policy.

There are no restrictions on the access to ‘Public’ information.

2.2.4. Policies and guidelines for use of accounts

Users are expected to become familiar with and abide by EzCloud policies, standards and guidelines for appropriate and acceptable usage of the networks and systems. This includes the acceptable use policy.

2.3 Access Control Methods

Access control methods used by default include:

- user account privilege limitations,
- servers and workstations access rights
- EzCloud user login rights
- Database access rights and ACLs
- Encryption at rest and in flight
- Any other methods as contractually required by interested parties.

Access control applies to all EzCloud-owned networks, servers, workstations, laptops, mobile devices and services run on behalf of EzCloud.

2.5 Penetration Tests

EzCloud's access control provision will be regularly made subject to penetration tests, in order to ascertain the effectiveness of existing controls and expose any weaknesses. Tests will include, where appropriate and agreed to, the systems of cloud service providers.

2.6 Further Policies, Codes of Practice, Procedures and Guidelines

This policy sits beneath EzCloud’s overarching Information Security Policy. Other supporting policies have been developed to strengthen and reinforce this policy

statement. These, along with associated codes of practice, procedures and guidelines are published together and are available for viewing on EzCloud's website. All staff and customers authorised to access EzCloud's network or computing facilities are required to familiarise themselves with these supporting documents and to adhere to them in the working environment.

2.7 Review and Development

This policy shall be reviewed and updated regularly by the ItCon if required to ensure that it remains appropriate in the light of any relevant changes to the law, organisational policies or contractual obligations.
Additional regulations may be created to cover specific areas.