Access Management Policy

Contents

1. Physical access

Access to the physical environment in which the organisation's assets are designed, created and maintained must be controlled appropriately.

Only authorised personnel that have a justified and approved business need are given access to restricted areas containing information systems or where data is processed.

Staff accesses buildings that house MENU's assets only using an access card. Other personnel must be granted access by a member of staff.

All access to parts of all buildings that the organisation occupies must be locked outside of normal office hours. The keys must be held only by those parties approved by a MENU Director.

MENU Technologies AG · Dammstrasse 19 · 6301 Zug, Switzerland · +41 41 723 2041 · hello@menu.app

All windows that open onto MENU's facilities must be lockable.

The last employee to leave the building at the close of business must ensure that the building is secure before leaving.

2. Electronic access

2.1 User access

The asset custodian must ensure that access to systems, services, data and information is restricted to authorised users who have a legitimate need to access the asset, in the context of their role in the organisation.

The asset custodian must ensure that each user is assigned a unique account to access an asset. The user must keep all the credentials associated with their accounts confidential.

The custodian of a system or service must regularly review the user accounts, groups and their permissions, to ensure that invalid accounts are not present, or have been disabled in preparation for removal, and that access rights are appropriate to users' roles.

The custodian of a system, service, data or information asset must provide authorised users only with the fewest privileges, rights and permissions to systems, services, data, information and resources that they need to fulfil their business role and associated duties.

2.2 Shared access

The custodian of an asset must approve the use of generic and shared accounts only rarely, where there is a specific business need, and no viable alternative. Only members of staff may be authorised to use a shared account. The approval must consider which specific members of staff may share the associated account.

A user may only use a shared account when sharing has been approved.

All digital credentials for a shared account must be stored in a password manager that has been approved by the Security Management, and access to those credentials must be limited to the set of staff for whom sharing has been authorised.

2.3 Privileged access

Privileged access applies to all individuals who have authorised administrative permissions and rights to access:

- computing systems, services, applications, network communication, EUDs; or
- the accounts, files, data, or processes of other users.

All administrative access to MENU systems, services or applications must be under strict control at all times.

The asset custodian is responsible for controlling administrative access to the asset. The custodian must inform Security Management of any authorised change to those who are granted privileged access.

The asset custodian must ensure that the scheme for administrative access sufficiently addresses disaster scenarios, including lack of availability of administrators.

Security Management may request the asset custodian to change administrative access to that asset where necessary, for example following a risk assessment, or when handling a security incident. The custodian must respond in a timely fashion to such a request.

2.4 Privileged credentials

Credentials that grant privileged access, or have the capability to set, change or disable privileged access are classified as <Sensitive> assets.

Any unplanned, or ad-hoc changes to who is granted or denied administrative access, or to the associated access-control groups, may result in disciplinary action.

The asset custodian must ensure that privileged access to the asset is audited, and must review access to the asset at least once a quarter.

2.5 Privileged access log

The audit log that records privileged access must be classified as a <Sensitive> asset and treated accordingly.

In particular, the asset custodian must ensure that the security of the audit process is sufficient to maintain integrity in the face of reasonably expected threats, and must grant Security Management read access to this audit log on request.

2.6 Application and system access

The asset custodian must control access, restricted only to those authorised users who have a legitimate business need, to:

- system utilities and program libraries, source code;
- installable programs; and
- the system that can build them from source code.

Only an authorised privileged user is able to install an application on a system, or change the configuration of a system.

2.7 Service access

Some assets depend on 3rd party services, such as cloud services.

The custodian of a service asset must ensure that access to the service asset is authorised through a user account, and complies with the current licence from the service supplier.

2.8 Hardware access

Where required by job role or function, and in consultation with Security Management, specific hardware are authenticated by MAC address on the network.

2.9 System perimeter access

The asset custodian ensures that the boundary between the business systems and the Internet or other non-trusted networks is protected by appropriate levels of security, i.e. firewalls and/or other endpoint protection measures.

2.10 Monitoring system access and use

Monitoring the organisation's systems and their use is important to MENU's security.

Failure to detect in a timely manner when an asset is being used inappropriately or by unauthorised parties could result in non-compliance with legal or regulatory requirements, and may result in attacks going unnoticed.

Therefore, the custodian of an asset must define the process to monitor the legitimate use of the asset before it is deployed, in consultation with Security Management, and based on a clear understanding of the risks to the asset.

The Risk Register must show where monitoring of an asset is judged to be insufficient.

MENU reserves the right to monitor systems or communications activity where it suspects that there has been a breach of policy in accordance with relevant legislations.

2.11 Leavers accounts

Whenever a member of staff leaves the MENU their line manager must inform HR and the Security Management of:

- their leaving date prior to them leaving; and
- again immediately once the member of staff no longer works for the organisation.

HR must ensure that all asset custodians have disabled all accounts to which the staff member was granted access within one day of leaving, and ensure that the leaver no longer has access to shared accounts or credentials.