Network Security Policy

Contents

1. Policy

- This policy sets out MENU's policy for the protection of the confidentiality, integrity and availability of the ICT network(s) and the resources it grants access to and seeks to ensure that MENU and its team members are able to make best use of the facilities offered by the ICT network(s), but do so in a way that is secure, complies with the law and is in the best interests of MENU, its team members and customers.

- To access network resources users will be issued with individual user credentials (typically username and password); these are issued for their sole use and must not be shared with other users. All passwords, PINs, and MFA QR Codes must be changed regularly and are to protected from disclosure at all times.

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

- Responsible departments (IT) will maintain up to date network diagrams (both logical and physical) that define the network topology, 'boundaries', IP addresses, core network equipment etc for all networks that they are responsible.

- Core network computer equipment will be housed in controlled and secure environments.

- Critical or sensitive network equipment will be protected by a secure perimeter, with appropriate security barriers and entry controls (including intruder alarms), fire suppression systems and in an environment that is monitored for temperature, humidity and power supply quality.

- IT will ensure that the network is permanently monitored to ensure performance is maintained, any faults are quickly identified/resolved and any potential security breaches are suitably acted on.

- No equipment is to be connected to any ICT network without the approval of those that manage/operate the ICT network concerned.

- Third party access to the ICT network(s) will be based on a formal contract and a separate Memorandum of Understanding (MoU) that both governs access and satisfies necessary security conditions.

- All external connections to the core MENU ICT network(s) are to mediated by appropriate access controls that protect against unauthorised or inappropriate access to the network and/or resources hosted on it. Such mediation will also control access and scan all authorised traffic via appropriate technical measures in order to protect the hosted resources.

- IT will ensure that where equipment is being disposed of all data on the equipment is securely overwritten.

- All potential security breaches on the ICT networks must be investigated and reported, as defined in MENU's Incident Management Policy.

2. Introduction

MENU is dependent upon its usage of ICT network(s) and AWS Infrastructure network(s) as a key tool for managing and delivering MENU Platform services and for communicating with its customers. However, the same features that make ICT useful (speed, ease-of-use, widespread access, ease of storage, etc.) also present risks to MENU, which must be managed to protect the MENU, its team members and customers. This document defines MENU's Network Security Policy which applies to all business functions and information contained/hosted on AWS (Amazon Web Services) or accessed via the MENU ICT network(s), the physical environment and administrators who support the network.

3. Scope

This policy applies to all MENU team members engaged in work for MENU, using ICT equipment connected to or via the MENU ICT network(s). This includes employees of organisations contracted to MENU.

4. Procedure

The overall Network Security Policy for MENU is described below and applies to **all ICT networks** used within MENU, regardless of who manages/operates them.

MENU's network(s)/AWS MENU Platform Infrastructure will be available when needed, can be accessed only by legitimate users and will contain complete and accurate information. The network must also be able to withstand or recover from threats to its availability, integrity and confidentiality. To satisfy this, MENU will undertake to the following:

- Protect all hardware, software and information assets under its control. This will be achieved by implementing a set of well-balanced technical and non-technical measures.
- Provide both effective and cost-effective protection that is commensurate with the risks to its network assets.
- Implement the Network Security Policy in a consistent, timely and cost effective manner.
- MENU will comply with other laws and legislation as appropriate.

4.1 Physical & Environmental Security

Responsible departments (IT Department for the core ICT network) will maintain up to date network diagrams (both logical and physical) that define the network topology, 'boundaries', IP addresses, core network equipment etc for all networks that they are responsible for.

Core network computer equipment will be housed in controlled and secure environments.

Critical or sensitive network equipment will be protected by a secure perimeter, with appropriate security barriers and entry controls (including intruder alarms), fire suppression systems and in an environment that is monitored for temperature, humidity and power supply quality. Such protection will normally be for the whole room; where this is not possible protection for individual equipment should be provided.

Entry to secure areas housing critical or sensitive network equipment will be restricted to those whose job requires it. The IT Department will maintain and periodically review a list of those with unsupervised access to core the MENU network/computer rooms.

The IT Department is responsible for ensuring that door lock codes for core MENU computer/network rooms are changed periodically, following a compromise of the code, if they suspect the code has been compromised.

Where servers are housed in non-ICT controlled/operated computer rooms such controls are to be exercised by the individual responsible for supporting such equipment(s).

Smoking, eating and drinking is forbidden in areas housing critical or sensitive network equipment.

All visitors to areas housing core critical or sensitive network equipment must be authorised by the IT Department and must be made aware of network security requirements. All visitors to these areas must be logged in and out. The log will contain name, organisation, purpose of visit, date, and time in and out. Visitors to rooms/areas that contain ICT switches and hubs are to be controlled by the IT Department. Responsible team members are to ensure that all relevant are made aware of procedures for visitors and that visitors are escorted, when necessary.

4.2 Access Control to the Network

Access to the network resources will be via a secure log-on procedure, designed to minimise the opportunity for unauthorised access.

Departmental managers and the IT Department must approve user access in accordance with this policy and relevant local guidance/process.

Access rights to the network will be allocated on the requirements of the user's role, rather than on a status basis.

Security privileges (i.e. 'superuser' or network administrator rights) to the network will be allocated on the requirements of the user's role, rather than on a status.

Access will not be granted until the IT Department registers a user. All users on the network will have their own individual user identification and password.

Users are responsible for ensuring their password is kept safe.

User access rights will be immediately removed or reviewed for those users who have left MENU or changed roles; managers must report all such occurrences to the IT department promptly.

a. Connecting Equipment or Providing New Services to the Network

No equipment is to be connected to any ICT network without the approval of those that manage/operate the ICT network concerned. Where new equipment or services are to be hosted on the network appropriate Risk Assessments are to be conducted prior to any such connection.

b. Wired Connection and Connection Points

In principle all network points are to be disabled unless they are actually in use or enabled to allow approved equipment to connected in the near term. Where areas are to be left unoccupied for periods in excess of a few days then network connectivity to the particular area is to be disabled until it is to be occupied again.

c. Wireless Connection and Wireless Access Points

New wireless connections should always be implemented with approved protocols and relevant security standards as defined by the IT department. Where Trust devices are permitted to access wireless networks rather than wired networks they are to be controlled in the same way that wired connections are.

Where 'guest' wireless services are offered on MENU premises devices provided by MENU are not permitted to make use of them.

'Guest' devices/services should always have appropriate controls configured to ensure proper separation of 'business' and 'non-business' data. Where provided these services are to maintain appropriate control of access to all resources and sufficient records to provide evidence of usage.

d. Security Standards for Wired or Wireless Devices

The IT department are to maintain seperate security (build) standards for all devices they are responsible for. These standards are to be applied to all equipments permitted to access the MENU network(s) whomever supports the equipment.

Where appropriate the IT department are to implement appropriate technical measures to provide Network Access Control on the MENU network.

e. Third Party Access Control to the Network

Third party access to the ICT network(s) will be based on a formal contract and a separate Memorandum of Understanding (MoU) that both governs access and satisfies necessary MENU company security conditions.

All third party access to the network must be logged, either as an individual one-off access or for more regular access in support of hosted applications/equipment. In the case of the later a register of such access is to be kept detailing the nature of the access.

Third party access is to be strictly limited to the equipment and functionality required to provide the contracted support required.

f. External Network Connections

All external connections to the core MENU ICT network(s) are to be mediated by appropriate access controls that protect against unauthorised or inappropriate access to the network and/or resources hosted on it. Such mediation will also control access and scan all authorised traffic via appropriate technical measures in order to protect the hosted resources.

Where external 'connections' are considered to be 'trusted', all new such connections are to be risk assessed prior to connection to ensure that they do not invalidate previous risk assessments on which controls and/or countermeasures are based.

In principle unsolicited network 'traffic' (excluding email traffic or approved 3rd party support access) that originates from outside the network boundaries should not be permitted to directly enter the internal network either to transit or to terminate. Appropriate technical measures should be implemented to ensure adequate separation of internal and external 'traffic'.

The IT Department must approve all connections to external networks and systems before they commence operation.

4.3 Data Backup and Restoration

The IT department is responsible for ensuring that backup copies of all data including the network configuration are taken regularly in accordance with IT local procedures and relevant SLAs such that services and data can be restored in accordance with requirements.

Documented procedures for the backup process and storage of backups will be produced and communicated to all relevant team members.

All backups will be stored securely and a copy will be stored in a separate location to the systems they originate from, preferably off-site but where this is not possible in a location that is a 'safe' distance from the originating systems themselves.

Where on line backups have been implemented in place of backups then similar separation between originating and backup locations must be implemented; under no cuircumstances are backups and original data to be kept in the same physical location(s).

Documented procedures for the safe and secure disposal of backup media will be produced and communicated to all relevant team members.

Users are responsible for ensuring that they save data to appropriate network shares where it is to be subject to centrally managed backup processes.

4.4 Reporting Security Incidents & Weaknesses

All potential security breaches on the ICT networks must be reported, as defined in MENU's Incident Mangement Policy.

4.5 Unattended Equipment and Clear Screen

Users must ensure that they protect the network from unauthorised access. They must log off the network when finished working.

MENU operates a clear screen policy that means that users must ensure that any equipment logged on to the network must be protected if they leave it unattended, even for a short time. Workstations must be locked or a screensaver password activated if a workstation is left unattended for a short time.

Users failing to comply will be subject to disciplinary action.