Access Management

User Account Provisioning

User Registration

1 All individuals having access to WHO systems and information assets must be registered through a formal registration process that selects and tracks the assignment of credentials and privileges.
2 The registration of a user account must be authorized by an officially designated authority.
3 Users should create their own credentials (see Password Management below).
4 Guidance should be provided on the generation of safe credentials, and a mechanism for the random generation of credentials should be provided.
5 The registration process must require users to verify their identity when creating or receiving credentials.
6 Credentials which are not set by the user must be generated automatically and be delivered to the user directly from the system which generates them. No user should ever provide credentials for another user.
7 Authorized users must be made aware of their responsibilities regarding information protection and, where required by procedures, sign an appropriate agreement.

Unique user account identity

8 A unique electronic identity will be assigned to each new user using a secure process.
9 Password sharing is forbidden.
10 Interactive login must be disabled for generic or service accounts (e.g. used by applications or databases).

Account de-provisioning

11 Access to all WHO systems cease with immediate effect when a user without a pending contract extension leaves the Organization. In that case, user accounts must be locked immediately and de-provisioned within 45 days.
12 Accounts which have not been used for more than 90 days in any system should be disabled and should remain disabled until manually reactivated.
13 Before de-provisioning an email account, an out-of-office automatic reply should be configured which sends a response which indicates that the user has left the organization and which offers alternative WHO contact details.
14 Privileges of any user can be revoked at any time in accordance with applicable Cybersecurity rules.

Authorization

Access control

15 All WHO information assets must have controls in place to ensure that the information is not improperly disclosed, modified, deleted or corrupted.

16 Standard operations procedures will be established at Headquarters and in all the Regions to define the exact process and roles in the user-identity management and provisioning in line with this rule and the Cybersecurity Policy.

17 Access controls will be used to limit user access to only those applications, data and functions which they need to perform their official duties (i.e. the "least-privilege" principle). Exceptions to this rule may be granted by the information/content owner based on business justification and must be documented and audited regularly.

18 Data specifically intended for public access must be segregated from "non-public" data (Internal Use or Confidential as defined in the WHO Information Classification Policy – see section XIV.2.3).

19 Permissions for all WHO information and technology assets must be set to a default which blocks access to unauthorized users (i.e. default deny).

20 Grants of Local Administrator permissions on end-user devices must strictly adhere to the Local Administrator Permissions Guideline in the End-User Device Management Related Document to ensure compliance with the Global Cybersecurity Policy.

Authentication

Secure Logon Procedures and Session Control

21 All controls and procedures specified in this document apply both to WHO Workforce accounts and to guest user accounts.

22 There is to be no distinction between different contract modalities in terms of login procedures and session control. To make such a distinction would mean that one group of users is more vulnerable than another, which would create a situation ripe for attack.

23 Systems shall not solicit user credentials but instead use the official WHO centralized identity provider (Single Sign-On), unless the use of local credentials is unavoidable in which that use is still subject to a risk exception approved by CISO or by another officer with signatory authority (D1+).

24 All systems requiring user authentication must adopt phishing resistant methods where feasible. Passkey based authentication using FIDO2 standards should be prioritized for interactive user access.

25 Legacy authentication methods such as SMS-based verification must be phased out. Only phishing resistant mechanisms, including Passkeys and approved TOTP based multifactor methods, may be used for user authentication.

Access to highly sensitive systems

26 Access to a highly sensitive system or network must not be allowed before users have been formally authenticated, authorized, and trained.

27 Access to highly sensitive systems must be carefully regulated and should be implemented using one of a class of technologies known as Privileged Access Management (PAM).

28 The PAM solution must support passkeys, ideally via integration with the WHO SSO system.

29 The PAM solution must support Session Management, Monitoring, and Recording. Sessions must be recorded and should be monitored by a member of the WHO workforce (staff or individual consultant) when a highly sensitive production system is accessed.

30 The PAM solution must support a Password Vault, and it must be used such that no one need be given access to highly privileged system accounts such as Administrator or root. No 3rd party user should have the password for such accounts, except via the break-glass mechanism in paragraph 37.

31 Privilege systems credentials must be automatically rotated on a regular basis. The PAM solution must be able to use the new credentials immediately.

32 The Vault system must have a failsafe break-glass feature, in which it can be accessed independently by senior IT officers, off-line.

33 Access to critical production systems must be exclusively granted Just-In-Time (JIT) based on a planned change and should only be available for a limited period during which the work is planned.

34 If the time to perform the work exceeds the allotted time in paragraph 33, then the change must be considered a failure, and reverted until another attempt can be scheduled.

35 The service owner of a sensitive system must perform a periodic review of access rights in that system, and must document that access review, and make it available for auditors.

36 Privileges must be revoked or reassessed upon job duties change.

37 Generic administration accounts (e.g. Local Administrator, root) must be limited to use in exceptional circumstances only, for example as break-glass accounts. Password sharing is prohibited.

38 Accounts with direct access to highly sensitive systems must never be used to perform regular business activities (e.g. email, web surfing, Office Automation).

Remote Access to On-Premises Systems

39 Remote access by 3rd parties to on-premises systems must follow all rules for remote access by WHO Staff and other workforce members and additionally must follow the rules in the following paragraphs.

40 All remote access by 3rd party suppliers must be via a Zero Trust Network Access (ZTNA) control tool which serves as a broker for all other systems, or via approved VPN devices. This includes access to end-user devices via end-user support services like LogMeIn.

41 Each user at a 3rd party supplier must have their own named user account for access to WHO systems regardless of how that access occurs.

Password Management

42 While stronger authentication methods are preferred, password authentication is still required for many systems and will probably be required in the indefinite future. Therefore, the following rules still apply when using passwords for authentication.

Initial password

43 Users must initialize their domain password via the self-service password system. For mobile devices, or when self-service initialization is not possible, users must be provided with an initial password (or PIN code for mobile devices) which they must change at the time of first login to any WHO system.

44 A domain password reset should be performed via the self-service system. In exceptional cases, should password reset be required by a Service Desk agent, the latter must identify and authenticate the user.

Password obfuscation

45 Systems or applications must only display the password in a clear text after a deliberate instruction from the user, and never as a default or initial state. It must be difficult to trigger the display of passwords in plain text accidentally.

Password strength

46 The key features of a strong password are uniqueness, length, and randomness.

47 Passwords must be unique. Systems should check with a WHO or external service to validate that a proposed user password has not been involved in a security breach.

48 It is difficult to enforce randomness, but length is easy to enforce. Therefore, systems must enforce password length. The minimum acceptable password length is 12 characters for most systems, or 20 characters for systems identified as elevated risk and for accounts with elevated privilege.

49 Service account passwords must be at least 24 characters long.

50 For passwords of fewer than 20 characters, systems must attempt to force randomness via rules concerning the complexity based on rules governing character sets and their use. These rules should be rotated frequently to prevent users from creating repeated patterns in their passwords.

51 Passwords of fewer than 20 characters must be changed at least every 60 days.