Identity and Access Management Policy

Document Owner:	RAS
Last Review Date:	March 2024
Version	1.1

Purpose

The purpose of the Cognition World Identity and Access Management Policy is to establish the requirements necessary to ensure that access to and use of Cognition World **Information Resources** is managed in accordance with business requirements, information security requirements, and other Cognition World policies and procedures.

Audience

The Cognition World Identity and Access Management Policy applies to individuals who are responsible for managing Cognition World Information Resource access, and those granted access privileges, including special access privileges, to any Cognition World **Information Resource**.

Contents

1. Access Control

- Access to Cognition World **Information Resources** must be justified by a legitimate business requirement prior to approval.
- Where multifactor authentication is employed, user identification must be verified in person before access is granted.
- Cognition World **Information Resources** must have corresponding ownership responsibilities identified and documented.
- Access to **confidential information** is based on a "need to know".
- Confidential data access must be logged.
- Access to the Cognition World network must include a secure log-on procedure.
- Workstations and laptops must force an automatic lock-out after a pre-determined period of inactivity.
- Documented user access rights and privileges to **Information Resources** must be included in disaster recovery plans, whenever such data is not included in backups.

2. Account Management

- All personnel must sign the Cognition World Information Security Policy Acknowledgement before access is granted to an account or Cognition World **Information Resources**.
- All accounts created must have an associated, and documented, request and approval.
- Segregation of duties must exist between access request, access authorization, and access administration.
- **Information Resource** owners are responsible for the approval of all access requests.

- User accounts and access rights for all Cognition World **Information Resources** must be reviewed and reconciled at least annually, and actions must be documented.
- All accounts must be uniquely identifiable using the user name assigned by Cognition World IT and include verification that redundant user IDs are not used.
- All accounts, including default accounts, must have a password expiration that complies with the Cognition World Authentication Standard.
- Only the level of access required to perform authorized tasks may be approved, following the concept of "least privilege".
- Whenever possible, access to **Information Resources** should be granted to user groups, not granted directly to individual accounts.
- Shared accounts must not be used. Where shared accounts are required, their use must be documented and approved by the Information Resource owner.
- User account set up for third-party **cloud computing applications** used for sharing, storing and/or transferring Cognition World **confidential** or **internal information** must be approved by the resource owner and documented.
- Upon user role changes, access rights must be modified in a timely manner to reflect the new role.
- Creation of user accounts and access right modifications must be documented and/or logged.
- Any accounts that have not been accessed within a defined period of time will be disabled.
- Accounts must be disabled and/or deleted in a timely manner following employment termination, according to a documented employee termination process.
- System Administrators or other designated personnel:
    - Are responsible for modifying and/or removing the accounts of individuals that change roles with Cognition World or are separated from their relationship with Cognition World.
    - Must have a documented process to modify a user account to accommodate situations such as name changes, accounting changes, and permission changes.
    - Must have a documented process for periodically reviewing existing accounts for validity.
    - Are subject to independent audit review.
    - Must provide a list of accounts for the systems they administer when requested by authorized Cognition World IT management personnel.
    - Must cooperate with authorized Cognition World Information Security personnel investigating security incidents at the direction of Cognition World executive management.

3. Administrator/Special Access

- Administrative/Special access accounts must have account management instructions, documentation, and authorization.
- Personnel with Administrative/Special access accounts must refrain from abuse of privilege and must only perform the tasks required to complete their job function.
- Personnel with Administrative/Special access accounts must use the account privilege most appropriate with work being performed (i.e., user account vs. administrator account).
- Shared Administrative/Special access accounts should only be used when no other option exists.
- The password for a shared Administrative/Special access account must change when an individual with knowledge of the password changes roles, moves to another department or leaves Cognition World altogether.

- In the case where a system has only one administrator, there must be a password escrow procedure in place so that someone other than the administrator can gain access to the administrator account in an emergency situation.
- Special access accounts for internal or external audit, software development, software installation, or other defined need, must be administered according the Cognition World Authentication Standard.

4. Authentication

- Personnel are required to maintain the confidentiality of personal authentication information.
- Any group/shared authentication information must be maintained solely among the authorized members of the group.
- All passwords, including initial and/or temporary passwords, must be constructed and implemented according to the following Cognition World rules:
    - Must meet all the requirements established in the Cognition World Authentication Standard, including minimum length, complexity and rotation requirements.
    - Must not be easily tied back to the account owner by using things like: user name, social security number, nickname, relative's names, birth date, etc.
    - Should not include common words, such as using dictionary words or acronyms.
    - Should not be the same passwords as used for non-business purposes.
- Password history must be kept to prevent the reuse of passwords.
- Unique passwords should be used for each system, whenever possible.
- Where other authentication mechanisms are used (i.e. security tokens, smart cards, certificates, etc.) the authentication mechanism must be assigned to an individual, and physical or logical controls must be in place to ensure only the intended account can use the mechanism to gain access.
- Stored passwords are classified as confidential and must be encrypted.
- All vendor-supplied default passwords should be immediately updated and unnecessary default accounts removed or disabled before installing a system on the network.
- User account passwords must not be divulged to anyone. Cognition World support personnel and/or contractors should never ask for user account passwords.
- Security tokens (i.e. Smartcard) must be returned on demand or upon termination of the relationship with Cognition World, if issued.
- If the security of a password is in doubt, the password should be changed immediately.
- Administrators/Special Access users must not circumvent the Cognition World Authentication Standard for the sake of ease of use.
- Users should not circumvent password entry with application remembering, embedded scripts or hard coded passwords in client software. Exceptions may be made for specific applications (like automated backup) with the approval of the Cognition World IT Management.
- If a password management system is employed, it must be used in compliance with the Cognition World Authentication Standard.
- Computing devices should not be left unattended without enabling a password protected screensaver or logging off of the device.
- Cognition World IT Support password change procedures must include the following:
    - authenticate the user to the helpdesk before changing password
    - change to a strong password
    - require the user to change password at first login.

- In the event that a user's password is compromised or discovered, the password must be immediately changed, and the security incident reported to Cognition World IT support.

5. Remote Access

- All remote access connections to the Cognition World networks will be made through the approved remote access methods employing data encryption and multi-factor authentication.
- Remote users may connect to the Cognition World networks only after formal approval by the requestor's manager or Cognition World Management.
- The ability to print or copy **confidential information** remotely must be disabled.
- Users granted remote access privileges must be given remote access instructions and responsibilities.
- Remote access to **Information Resources** must be logged.
- Remote sessions must be terminated after a defined period of inactivity.
- A secure connection to another private network is prohibited while connected to the Cognition World network unless approved in advance by Cognition World IT management.
- Non-Cognition World computer systems that require network connectivity must conform to all applicable Cognition World IT standards and must not be connected without prior written authorization from IT Management.
- Remote maintenance of organizational assets must be approved, logged, and performed in a manner that prevents unauthorized access.

6. Vendor Access

- Vendor access must be uniquely identifiable. and comply with all existing Cognition World policies.
- External vendor access activity must be monitored.
- All vendor maintenance equipment on the Cognition World network that connects to the outside world via the network, telephone line, or leased line, and all Cognition World Information Resource vendor accounts will remain disabled except when in use for authorized maintenance.

Enforcement

Personnel found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, and related civil or criminal penalties.

Any vendor, consultant, or contractor found to have violated this policy may be subject to sanctions up to and including removal of access rights, termination of contract(s), and related civil or criminal penalties.

References

- ISO 27002: 6, 7, 8, 9, 12, 15
- NIST CSF: PR.AC, PR.IP, PR.MA, PR.PT, DE.CM
- Cognition World Information Classification and Handling Policy
- Cognition World Disaster Recovery Policy

Waivers

Waivers from certain policy provisions may be sought following the Cognition World Waiver Process.

Version History

Version	Modified Date	Approved Date	Approved By	Reason/Comments
1.0.0	November 2022	November 2022	RAS	Document Origination
1.1	March 2025	March 2025	TDM	Document update