

Document Index & Conventions

Lists every UAC document and sets the rules all of them follow.

Document information

Item	Value	Meaning
Unit	UAC	Unified Admission Coordination Unit
Area	GEN	General: applies to the whole document set
Document type	STD	Standard: how things are set up and run
Number	01	Sequence within the same unit, area and type
Version	0.2	Draft
Classification	Internal	Ministry staff. Not shared outside the ministry
Owner	Eng. Ahmad Abd Al-Hadi, UAC	Responsible for this document
Next review	Set at first approval, every 6 months after	Every 6 months, and straight after any incident or major change that touches the document
JNCSF controls	1, 2, 59, 60, 226, 322, 432, 433, 438, 439	Policy management
Document code	UAC-GEN-STD-01	Unit-Area-Type-Number. Never changes; the version is tracked separately

Approval

Role	Name · Position	Decision	Date & time	Signature	Signed file reference
Prepared by	Eng. Ahmad Abd Al-Hadi · Computer Engineer				
Reviewed by					
Approved by					

Signatures apply to a frozen PDF of one exact version. Decision is Approved or Returned with comments. Signed file reference is the version plus the SHA-256 fingerprint of the signed PDF.

Revision history

Version	Date	Change	By
0.1	18 Oct 2026	New document under JNCSF. Replaces the earlier draft index, which is kept as reference only.	Eng. Ahmad Abd Al-Hadi
0.2	19 Oct 2026	Added job title as a shared variable; confirmed owner meaning, status column, area descriptions and column names	Eng. Ahmad Abd Al-Hadi

Purpose & scope

Entry point to every technical document of the Unified Admission Coordination Unit (UAC). Lists each document with its code and status, and sets the rules for coding, layout, versioning, review, signatures, classification, secrets and writing.

Covers the UAC production environment: infrastructure, storage, backup and disaster recovery, access and security, developer rules.

Every document is based on the Jordan National Cybersecurity Framework (JNCSF) issued by NCSC. All documents are in English.

Related documents

- Cybersecurity Policy (UAC-GEN-POL-01): the policy this standard serves
- Control Applicability List (UAC-GEN-REC-04): which JNCSF controls apply to UAC and why

Coding scheme

Every document code has four parts: Unit-Area-Type-Number, for example UAC-DR-PLN-01. Every document has a plain title for reading and a code for reference. The code never changes; the version is tracked separately.

Unit. UAC. Other units or buildings get their own code later.

Code	Unit
UAC	Unified Admission Coordination Unit

Area.

Code	Area	Covers
GEN	General	index, policies, registers, procedures for every area
INF	Infrastructure	hosts, VMs, network, storage
DR	Backup and disaster recovery	
SEC	Access and security	
DEV	Developer rules	

Type.

Code	Type	Meaning
POL	Policy	the rules and who must follow them
STD	Standard	how things are set up and run
PLN	Plan	what happens in a defined situation, such as continuity or recovery
SOP	Procedure	step-by-step actions
REC	Record	logs, registers, inventories, test results

Number. 01, 02 ... within the same unit, area and type.

A retired document keeps its code with status Superseded; codes are never reused.

Document register

Statuses: Planned, Draft, In review, Approved, Superseded.

Document	Area	Type	Status	Code
Document Index & Conventions	General	Standard	Draft	UAC-GEN-STD-01
Cybersecurity Policy	General	Policy	Planned	UAC-GEN-POL-01
Change Register	General	Record	Planned	UAC-GEN-REC-01
Action Register	General	Record	Planned	UAC-GEN-REC-02
Incident Log	General	Record	Planned	UAC-GEN-REC-03
Control Applicability List	General	Record	Planned	UAC-GEN-REC-04
Incident Procedure	General	Procedure	Planned	UAC-GEN-SOP-01
Infrastructure & Sizing	Infrastructure	Standard	Planned	UAC-INF-STD-01
Storage Design	Infrastructure	Standard	Planned	UAC-INF-STD-02
Asset & Configuration Inventory	Infrastructure	Record	Planned	UAC-INF-REC-01
Backup Policy	Backup & DR	Policy	Planned	UAC-DR-POL-01
Continuity Plan	Backup & DR	Plan	Planned	UAC-DR-PLN-01
Backup & DR Design	Backup & DR	Standard	Planned	UAC-DR-STD-01
Job Cards	Backup & DR	Standard	Planned	UAC-DR-STD-02
Hardware & Malware Recovery	Backup & DR	Procedure	Planned	UAC-DR-SOP-01
Recovery Test Records	Backup & DR	Record	Planned	UAC-DR-REC-01
Access & Secrets Policy	Access & Security	Policy	Planned	UAC-SEC-POL-01
Accounts & Access Register	Access & Security	Record	Planned	UAC-SEC-REC-01
Developer Rules	Developer	Policy	Planned	UAC-DEV-POL-01

Notes:

- The Incident Procedure (UAC-GEN-SOP-01) follows NCSC's 2023 incident categorization instructions.
- The Asset & Configuration Inventory (UAC-INF-REC-01) (inventory.yml) is the single source for server, pool, share and job names in every document.

Versioning

Start at 0.1, then 0.2, 0.3 ... while drafting; 1.0 at first approval; 1.1, 1.2 ... for content updates; 2.0 for a redesign. Every change gets a revision-history row.

Review

Every 6 months, and straight after any incident or major change that touches the document. The review date is recorded even when nothing changes.

Signatures

1. The approved version is exported to PDF and frozen.
2. The SHA-256 of that PDF is recorded as the signed file reference.
3. The PDF is signed, by hand now or digitally later.
4. Any edit after signing means a new version and a new signature.

Offline copy

A printed, signed copy of every approved document is kept in the vault.

Classification

Classification follows JNCSEF controls 147–150. It is set by the owner at creation and checked at every review.

Level	Who may see it	Handling	If leaked	Examples
Public	Anyone	No limits	No harm	None today
Internal	Ministry staff	Not shared outside the ministry	Minor	Index & Conventions, policies, Developer Rules
Confidential	UAC technical staff and named approvers (by role)	Need-to-know; printed copies kept locked	Helps an attacker plan: IPs, server names, network layout	Design documents, Job Cards, Continuity Plan, Asset & Configuration Inventory
Highly Confidential	Named individuals only	Locked storage; every access or opening logged	Gives direct access or exposes people	Accounts & Access Register; the break-glass envelope

Confidential and Highly Confidential documents are never published on a public website.

Secrets

No document contains a password, key or other secret, in text or in a blank field. A document names the account and the password-manager entry that holds its secret. Full rules go in Access & Secrets Policy (UAC-SEC-POL-01).

- Passwords live in a password manager hosted on both TrueNAS servers, one replicating the other; the tool is still to be chosen.
- A break-glass set of passwords is printed, sealed and signed in an envelope, kept in the vault in the management office, used only when a staff member with access cannot be reached.
- Every opening is logged; the passwords in it are changed after any opening.

Writing conventions

Topic	Rule
Times	12-hour AM/PM, local Amman time, e.g. 8:00 PM.
Dates	18 Oct 2026 format.
Measured durations	Rounded up to the next 15 minutes.
Names	Exactly as in the live system, from inventory.yml.
Values	The exact value in every table cell; never “same” or “as above”.
Capacity	Disk sizes in TB as sold; usable space, quotas, volumes in TiB / GiB.
Secrets	Never written; name the account and its password-manager entry.
Cross-references	Title, code and section, e.g. “see Storage Design (UAC-INF-STD-02), Zvols”.