المركز الوطني للأمن السيبراني

قرار رقم (2) لسنة 2026

بشأن الضوابط الوطنية الأساسية للأمن السيبراني

رئيس المركز الوطني للأمن السيبراني

– بعد الاطلاع على المرسوم رقم (37) لسنة 2022 بشأن إنشاء المركز الوطني للأمن السيبراني،

– وعلى قرار مجلس الوزراء رقم (117) لسنة 2022 بتحديد الوزير المشرف على المركز الوطني للأمن السيبراني،

– وعلى قرار مجلس الوزراء الموقر رقم (166) لسنة 2025، بتعيين رئيس المركز الوطني للأمن السيبراني،

– وعلى القرار رقم (35) لسنة 2023 بشأن الإطار الوطني لحوكمة الأمن السيبراني،

– وعلى القرار رقم (1) لسنة 2025 بشأن لائحة الإطار الوطني العام لتصنيف البيانات،

– وبناء على ما تقتضيه مصلحة العمل،

قرر ما يلي:

مادة (1) التعاريف

- المركز: المركز الوطني للأمن السيبراني.
- الجهات المعنية: الجهات الحكومية المدنية والعسكرية والأمنية ومؤسسات القطاع الخاص داخل دولة الكويت ذات الصلة باختصاصات المركز، والجهات التي يحددها المركز وفقا لأحكام المرسوم رقم 37 سنة 2022.
- الضوابط الوطنية الأساسية للأمن السيبراني: الملحق المعتمد بموجب هذا القرار، والمتضمن الحد الأدنى الوطني من الضوابط والمتطلبات الأساسية للأمن السيبراني الصادرة عن المركز.
- الإدارة العليا: القيادات العليا في الجهة المعنية، وفق الهيكل التنظيمي المعتمد لها، ممن يملكون صلاحية التوجيه والاعتماد وتخصيص الموارد والإشراف على التنفيذ، ويشمل ذلك رئيس الجهة أو من في حكمه، ووكلاء الجهة والوكلاء المساعدين أو من في حكمهم.
- الملحق: الملحق رقم (1) المرفق بهذا القرار بعنوان (الضوابط الوطنية الأساسية للأمن السيبراني في دولة الكويت)، (Kuwait National Basic Cybersecurity Controls).
- المتطلبات الإلزامية: الأحكام أو المتطلبات الواردة في الملحق بصيغة الوجوب، والتي يجب على الجهة المعنية تنفيذ ما ينطبق منها بحسب طبيعة أعمالها وأصولها، وأنظمتها وبياناتها وخدماتها.
- الاستثناء: موافقة موثقة ومحددة المدة على عدم تطبيق متطلب إلزامي محدد من متطلبات الملحق، على أن تتضمن المبرر، ونطاق الاستثناء، ومدته، والضوابط التعويضية متى اقتضى الأمر.

مادة (2) الغرض

يهدف هذا القرار إلى اعتماد ونشر الضوابط الوطنية الأساسية للأمن السيبراني في دولة الكويت بوصفها الحد الأدنى الوطني الواجب تطبيقه من الجهات المعنية، وذلك لتحقيق ما يلي:

- رفع مستوى الجاهزية والمرونة السيبرانية على المستوى الوطني.
- حماية الأصول والأنظمة والشبكات والخدمات والبيانات من المخاطر والتهديدات السيبرانية.
- تعزيز الحوكمة والمساءلة وإدارة المخاطر والامتثال في الجهات المعنية.
- توحيد الحد الأدنى من المتطلبات الإلزامية الواردة في الملحق، بما يتيح قياس مستوى الالتزام بها وإثباته ومتابعته من قبل المركز.

مادة (3) النطاق

تطبق أحكام هذا القرار والملحق المرفق به على الجهات المعنية وفقاً لأحكام المرسوم رقم (37) لسنة 2022.

مادة (4) الالتزام

- تلتزم الجهات المعنية بتطبيق الضوابط الوطنية الأساسية للأمن السيبراني الواردة في الملحق المرفق بهذا القرار، واتخاذ ما يلزم لتنفيذ المتطلبات الإلزامية التي تنطبق عليها خلال المدد الزمنية المحددة فيه.
- تلتزم الجهات المعنية بتوفير الحلول والأدوات التقنية اللازمة لدعم تنفيذ المتطلبات الإلزامية الواردة في الملحق، بما يمكن من متابعتها وإثبات الالتزام بها، وذلك بما يتناسب مع طبيعة أعمال الجهة وأصولها، وأنظمتها وبياناتها وخدماتها.
- تلتزم الجهات المعنية بإجراء تقييم ذاتي دوري، وبحد أدنى مرة واحدة سنويا، لقياس مدى الالتزام بالملحق المرفق، وذلك باستخدام النماذج أو القوائم التي يعتمدها المركز لهذا الغرض.
- تلتزم الجهات المعنية بالاحتفاظ بالسجلات والوثائق والأدلة اللازمة لإثبات مستوى الالتزام، وتقديمها إلى المركز عند الطلب، كما تلتزم بتقديم ما يلزم من معلومات ووثائق إلى الجهات المختصة الأخرى متى كان ذلك مطلوباً وفقاً للقوانين والنظم واللوائح المعمول بها.
- تلتزم الجهة المعنية باعتماد وتطبيق الإجراءات والسياسات الداخلية اللازمة لتنفيذ المتطلبات الإلزامية الواردة في الملحق، وضمان التزام العاملين لديها بها، واتخاذ ما يلزم حيال أي مخالفة وفقًا للأنظمة واللوائح المعمول بها.
- إذا كانت الجهة المعنية خاضعة لمتطلبات تنظيمية أو رقابية قطاعية أخرى، فتلتزم بالمتطلبات الأشد، مع عدم الإخلال بأحكام هذا القرار واختصاصات المركز.
- لا يجوز الخروج على أي من المتطلبات الإلزامية الواردة في الملحق إلا بموجب استثناء موثق ومحدد المدة ومبرر بالمخاطر، ووفقًا لأحكام هذا القرار والملحق المرفق به، مع بيان الضوابط التعويضية متى اقتضى الأمر.

مادة (5) الإشراف والمتابعة

• تتولى الإدارة العليا في الجهة المعنية توفير واعتماد ما يلزم من أدوار ومسؤوليات وموارد وإجراءات داخلية لضمان تنفيذ أحكام هذا القرار والالتزام به.

• يتولى المركز الإشراف على تنفيذ هذا القرار ومتابعة مدى الالتزام به، وله في سبيل ذلك طلب نتائج التقييم الذاتي وما يلزم من تقارير وسجلات وأدلة، وإجراء ما يلزم من فحص لمدى التزام الجهة المعنية بأحكام هذا القرار والمتطلبات الواردة في الملحق وقياس مستوى الامتثال لها.

مادة (6) الملحق والأدوات المساندة

• يعد الملحق رقم (1) المرفق بهذا القرار بعنوان (الضوابط الوطنية الأساسية للأمن السيبراني)، (Kuwait National Basic Cybersecurity Controls). جزءًا لا يتجزأ من هذا القرار، ويعمل به مع أحكامه.

• يبقى الملحق المرفق بهذا القرار باللغة الإنجليزية، ويعتد به بوصفه النص الفني المعتمد للضوابط الوطنية الأساسية للأمن السيبراني.

• يجوز للمركز إصدار ملاحق، أو مرفقات، أو أدلة استرشادية، أو نماذج، وغيرها من الوثائق أو الأدوات المكملة، وذلك لدعم تنفيذ هذا القرار والملحق المرفق به.

• وتعد جميع ملاحق، أو مرفقات، أو أدلة استرشادية، أو نماذج، وغيرها من الوثائق أو الأدوات التي يصدرها المركز تنفيذًا لهذا القرار، مكملة له وللملحق المرفق به، وتفسر وتطبق بما يحقق الاتساق والتكامل بينها. ولا يترتب على إصدار أي منها تعديل أو إلغاء أو استبدال أي حكم من أحكام هذا القرار أو الملحق إلا بقرار لاحق يصدر عن المركز وينص صراحة على ذلك. وعند تعذر التوفيق، تكون العبرة بأحكام هذا القرار والملحق المرفق به، ما لم يرد نص صريح في القرار اللاحق بخلاف ذلك.

مادة (7) توفيق الأوضاع والإنفاذ

تلتزم الجهات المعنية بتوفيق أوضاعها وتحقيق الالتزام الكامل بالمتطلبات الإلزامية التي تنطبق عليها خلال مدة زمنية لا تتجاوز (18) شهراً من تاريخ نشر هذا القرار في الجريدة الرسمية، ما لم يمنح المركز، بناءً على طلب مسبب من الجهة المعنية، استثناءً موثقاً ومحدد المدة وفقاً لأحكام هذا القرار والملحق المرفق به.

مادة (8) تاريخ النفاذ

يعمل بأحكام هذا القرار من تاريخ نشره في الجريدة الرسمية.

مادة (9) الإلغاء والتعديل

يلغى كل نص أو حكم يتعارض مع أحكام هذا القرار، ويجوز تعديل هذا القرار أو الملحق المرفق به بقرار لاحق من المركز متى اقتضت مصلحة العمل ذلك.

رئيس المركز الوطني للأمن السيبراني

صدر في: 31مارس2026م

Annex (1) to Decision No. 2 of 2026
Kuwait National Basic Cybersecurity Controls

1. Introduction

The State of Kuwait recognizes that a strong cybersecurity posture is essential to protect national interests, public services, economic stability, and the safety of citizens and residents.

Amiri Decree No. 37 of 2022 established the National Cyber Security Center (NCSC) as the competent national authority for cybersecurity.

At a strategic level, NCSC's objectives include building and developing an effective national cybersecurity ecosystem; protecting vital interests and critical infrastructure; strengthening national cybersecurity capabilities; promoting a national cybersecurity culture; and enabling cooperation, coordination, and information sharing with relevant local and international stakeholders.

To achieve these objectives, NCSC is mandated to develop and issue national cybersecurity strategies, policies, standards, and implementation mechanisms; establish governance and national plans to address cyber risks and threats; coordinate cybersecurity operations and incident response, and provide support and guidance where needed; and conduct assessments and audits to verify compliance with issued requirements.

Entities are obligated to maintain cybersecurity in a manner consistent with NCSC's mandate; implement NCSC-issued strategies, policies, standards, and controls; promptly notify NCSC of actual or suspected cybersecurity threats or incidents; provide the documents, information, and access necessary to enable NCSC oversight; and comply with applicable requirements in the National Data Classification Framework (Decision No. 1 of 2025).

This document sets out a minimum cybersecurity baseline that Entities MUST implement as essential cyber hygiene.

This baseline forms Annex (1) to Decision No. 2 of 2026 concerning the National Basic Cybersecurity Controls in the State of Kuwait.

this baseline. Entities MUST be able to demonstrate their level of implementation of this baseline to NCSC upon request. Entities MUST also provide such information to other competent authorities where required under applicable law or sector-specific regulation.

3. Scope and Applicability

This baseline, as Annex (1) to Decision No. 2 of 2026, applies to all Entities that fall under the mandate of NCSC as defined in Amiri Decree No. 37 of 2022 regarding the establishment of NCSC.

Other public and private Entities not formally within this mandate are strongly encouraged to adopt this baseline on a voluntary basis in the interest of the resilience, safety, and economic stability of the State of Kuwait.

4. Use of this Baseline

This baseline defines the national minimum cybersecurity controls that Entities MUST implement.

Entities MAY implement stronger or additional controls where required by their risk profile, legal obligations, sector-specific requirements, or the sensitivity and criticality of the systems, services, and data they manage.

This baseline is intended to establish a common national minimum level of cybersecurity and does not limit Entities from adopting more advanced or additional safeguards where appropriate.

In this baseline:

MUST – indicates a mandatory requirement;

SHOULD – indicates a recommended practice; and

MAY – indicates an optional practice.

5. Control Structure

The controls in this baseline are grouped by NIST CSF functions:

- GOV – Govern: Establish and monitor the Entity's cybersecurity risk management strategy, expectations, and policy.
- ID – Identify: Determine the current cybersecurity risk to the Entity.
- PR – Protect: Prevent or reduce cybersecurity risks.

The baseline is:

- Aligned with recognized international frameworks, particularly the CIS Controls v8.1 – Implementation Group 1 (IG1) and the NIST Cybersecurity Framework (CSF).
- Referenced to the National Data Classification Framework (Decision No. 1 of 2025).
- Risk-oriented and practical, designed for Entities with limited cybersecurity resources.
- Intended as a starting point, not an end state. Entities can later build on this baseline with more advanced controls as their maturity increases.

This baseline aligns with Kuwait's national cybersecurity mandates, including the National Cybersecurity Governance Framework (Decision No. 35 of 2023), the National Data Classification Framework (Decision No. 1 of 2025), and Amiri Decree No. 37 of 2022 establishing NCSC.

2. Objectives

- Establish a national baseline.

Define realistic, implementable minimum controls that Entities MUST adopt to achieve a common level of cybersecurity hygiene and to protect the confidentiality, integrity, and availability of Entity assets.

- Align with international best practice.

Ensure that the baseline is consistent with widely recognized international frameworks and guidance, such as CIS Controls v8.1 and NIST CSF, while allowing adaptation to Kuwait's regulatory and operational context.

- Promote accountability and risk management.

Require Entities to assign clear responsibilities, maintain policies and procedures, classify their data, manage service providers, and document compliance so that cybersecurity risks are identified, owned, and managed in a structured way.

- Enable measurable compliance.

Ensure that implementation can be measured at least through periodic self-assessment against

GOV–3	Data Classification & Sovereignty	Ensure data is handled according to its sensitivity and legal requirements.	Implement a data classification program aligned with the National Data Classification Framework, using at least Sensitive, Restricted, and Public categories, with clear criteria and examples. Issue a Data Classification Policy/Document approved by senior management and submitted to NCSC for approval, in accordance with Decision No. 1 of 2025. Tag or label data (and related systems/records) with its classification and ensure protection measures increase with sensitivity (for example: stronger access controls and encryption for Sensitive data). Storing or processing Sensitive data outside Kuwait MUST follow the national approval process and receive explicit NCSC approval before use (per applicable regulations).
GOV–4	Kuwaitization & Vetting for Cyber Roles	Support national capacity building and reduce insider risk in critical cyber roles.	For key cybersecurity roles (e. g., SOC analysts, administrators, incident responders), prioritize qualified Kuwaiti nationals where feasible and consistent with national HR frameworks and local laws and regulations. For staff in such sensitive roles, perform basic pre–employment screening (e.g., identity verification, employment history, conflict–of–interest checks) in line with applicable laws and HR policies. Maintain a simple list of designated "sensitive cyber roles" and ensure screening is documented.

- **DE – Detect: Find and analyze possible cybersecurity attacks and compromise.**
- **RS – Respond: Take action regarding a detected cybersecurity incident.**
- **RC – Recover: Restore assets and operations that were impacted by a cybersecurity incident.**

Each control table below uses the following fields:

- **Control ID – Unique identifier;**
- **Control Title – Short descriptive name;**
- **Purpose / Description – What risk or need it addresses; and**
- **Minimum Requirement – Simple, auditable expectation.**

6. GOVERN (GOV) – Governance, Roles and Policies

Control ID	Control Title	Purpose / Description	Minimum Requirement
GOV–1	Governance & Roles	Establish clear accountability for cybersecurity.	The entity MUST designate an employee at manager level or above with overall responsibility for cybersecurity. Define and document roles and responsibilities for information security, IT operations, risk management, data classification, and incident response. Review and update this structure at least annually or when major organizational changes occur.
GOV–2	Policies & Exception Management	Ensure behavior and decisions are guided by documented, approved rules.	Maintain core written policies that, at minimum, cover: acceptable use, Secure Configuration, data classification, access control, backup & recovery, incident response, and third–party / service provider security. Policies SHOULD be approved by management and reviewed at least every two years. Any deviations MUST follow a simple exception process with documented risk acceptance and an expiry date.

			location, purpose, criticality, and lifecycle state (in use, spare, retired). For physical assets, use unique, machine-readable labels (e.g., barcode/QR-style) to support scanning and tracking. At least weekly, review network discovery or similar tools to identify unauthorized devices and either remove, block, or formally approve them.
ID-2	Software & Provider Inventory	Maintain visibility of software in use and service providers.	Maintain a list of authorized software (including version families) and service providers (including cloud and SaaS). At least monthly, review systems for unauthorized software and either remove it or record a documented exception. The list register SHOULD include owner, contact details, service description, criticality, and data sensitivity (which classifications are processed). Review provider information at least annually.
ID-3	Data & Account Inventory	Understand what data and accounts exist and who owns them.	Maintain an inventory of critical and sensitive data sets, including classification, location, and business owner. Maintain an inventory of user and service accounts including privileges and last activity. Review accounts at least quarterly. Disable or remove dormant interactive user accounts that have not been used for 90 days, where the technology supports it. Review service accounts at least quarterly to validate continued business need. Ensure high-risk or privileged accounts are clearly identified.

8. PROTECT (PR) – Configuration, Access, Awareness, Protection and Backup

8.1 PR-1 Secure Configuration, Hardening & Network Segmentation

Control ID	Control Title	Purpose / Description	Minimum Requirement
PR-1	Secure Configuration & Hardening	Reduce the attack surface of systems and devices.	Establish hardened configuration baselines for servers, workstations, network devices, and key applications. From this baseline, disable or remove services, features and ports that are not

GOV-5	Periodic Self-Assessment & Continuous Improvement	Provide a minimal mechanism to measure implementation of this baseline.	At least once per year, complete a self-assessment against this baseline using an NCSC-issued or NCSC-approved checklist. Document the results, key gaps, actions, and target dates. Retain the record for at least three years and make it available to NCSC upon request. Use major incidents or audits to update priorities.
GOV-6	Service Provider & Outsourcing Governance	Manage cybersecurity risk arising from external providers, including cloud.	Establish and maintain an inventory of service providers (including cloud/managed services), including classification and an entity contact for each provider; review at least annually or upon significant change. • For service providers handling Sensitive data or supporting critical services, document the service scope and shared responsibilities for protecting the service and data. • Ensure incident response contact information includes relevant service providers, and define incident reporting timeframes and mechanisms for provider-related incidents. • For offboarding/termination, ensure required actions are performed to remove access and handle data appropriately, retaining evidence where applicable.

7. IDENTIFY (ID) – Assets, Software, Data and Accounts

Control ID	Control Title	Purpose / Description	Minimum Requirement
ID-1	Asset & Service Inventory	Maintain an up-to-date view of hardware and key services.	Maintain a central electronic inventory of hardware assets (servers, workstations, laptops, network equipment, IoT/OT devices, etc.) and key on-premises services. Record at least: owner,

			apply operating system and application patches at least monthly on supported systems. Keep records of scans and key remediation actions.

8.2 PR–2 Identity, Authentication & Password Hygiene

Control ID	Control Title	Purpose / Description	Minimum Requirement
PR–2	Identity, Authentication & Password Hygiene	Ensure access is properly controlled and accounts are harder to compromise.	Require unique passwords for all accounts; do not reuse the same password across different systems. As a simple rule, require at least 8 characters for accounts protected by multi–factor authentication (MFA) and at least 14 characters for accounts without MFA. Avoid forcing regular password changes unless compromise is suspected. Enforce session lock or screen saver after 15 minutes of inactivity for workstations and around 2 minutes for mobile devices where practical. Limit administrator privileges to dedicated admin accounts, and require staff to perform day–to–day activities (email, web browsing, office work) from a normal user account. Implement MFA for all remote network access, externally exposed applications, and privileged/admin accounts where supported, using at least two different types of factor (something you know, something you have, something you are).

PR–2 – Additional baseline requirements

Control ID	Control Title	Purpose / Description	Minimum Requirement
PR–2.1	Corporate Email Only & Personal Email Ban	Ensure work communications use managed, auditable channels and reduce data	Require that all official business communications use only Entity–approved corporate email
			needed for the system's role. Change or disable default accounts and default passwords. Enable a host–based firewall on endpoints and servers and allow only the network traffic required for normal operation. Review configurations at least annually and after major changes.
PR–1.1	Network Segmentation	Limit the spread and impact of attacks by separating networks.	Where feasible, separate user networks from server/data networks, and keep management/admin interfaces on a more restricted network segment. Place internet–facing systems in a more controlled network zone. Avoid direct access from user networks to sensitive servers unless explicitly required and approved. • Do not treat network location alone as sufficient basis for trust. Access to management/admin interfaces and Critical Systems MUST be explicitly authorized based on least privilege and protected with strong authentication in accordance with PR–2 (including MFA for administrative access where supported). • Document such access and review it at least annually.
PR–1.2	Vulnerability Management & Patching	Identify and address technical weaknesses in a structured way.	Have a simple written process for vulnerability management and review it at least annually. Run automated vulnerability scans on key systems: at least monthly for internet–facing systems, at least quarterly for other important internal systems, and after major changes. After each scan, review the report, produce a short action list, and fix the most serious issues first (for example, high and critical findings). Aim to

			and how to report suspicious activity or incidents. Use simple language and relevant examples.
Control ID	Control Title	Purpose / Description	Minimum Requirement
PR-3.1	Official Social Media & Digital Presence	Ensure official accounts are authentic, protected, and clearly distinguished from impostors.	Maintain a central register of official Entity accounts on external platforms (e. g., major social networks, video platforms). Create official accounts using corporate email addresses and appropriate naming conventions. Where the platform provides it and criteria are met, enable verification or "official" status. Protect these accounts with MFA and role-based administration; review access at least annually and remove access when staff leave or change roles.

8.4 PR-4 Malware, Email & Web Protection

Control ID	Control Title	Purpose / Description	Minimum Requirement
PR-4	Malware, Email & Web Protection	Reduce the risk of malware and phishing attacks.	Deploy endpoint protection (e. g., anti-malware/EDR software) on supported servers and workstations with automatic updates and centralized alerting where possible. Use email and web security controls (e.g., spam filtering, attachment and URL filtering) to block common malicious content and clearly suspicious file types. Configure email systems to block or warn on dangerous file extensions that are not needed for business and to limit very large attachments
			leakage via personal email.	accounts on approved domains. Personal/consumer email accounts MUST NOT be configured on corporate devices and MUST NOT be used for work-related communication. Enforce this via (1) an acceptable use policy, and (2) device and email configuration (e.g., MDM or mail client settings) that prevent adding personal accounts where feasible.
PR-2.2	Password Manager & Credential Hygiene	Help staff maintain strong, unique passwords without reuse.	Provide or approve a password-manager-style solution for staff who manage multiple credentials. Encourage use of long, unique passwords generated by the manager for each system. For shared/team accounts (where unavoidable), use shared password vaults or similar capabilities; do not share passwords through email, chat, or on paper.

8.3 PR-3 Awareness & Human Factors

Control ID	Control Title	Purpose / Description	Minimum Requirement
PR-3	Security Awareness & Training	Build a basic culture of secure behavior.	Establish a security awareness program and provide training at least annually and for new joiners. At minimum, cover: social engineering and phishing, safe use of email and the web, handling of Sensitive and Restricted data, password and MFA hygiene, use of approved communication tools, use of portable media,

			Entity systems, especially those handling Sensitive data. Establish procedures to allow only authorized portable media if necessary for business, and train staff on proper usage of portable media devices.

8.5 PR–5 Data Protection, Backup & Lifecycle

Control ID	Control Title	Purpose / Description	Minimum Requirement
PR–5	Data Protection, Backup & Lifecycle	Ensure critical data is appropriately protected, can be restored, and is disposed of safely.	Implement regular, automated backups for critical systems and data, with priority to Sensitive and Restricted data. Store backups in at least one separate location (for example, a separate network segment, storage system, or cloud account). Protect backup data from unauthorized access and tampering (e.g. access controls, encryption). Test restoration of backups for key systems at least annually. Define and apply retention periods and secure disposal procedures aligned with legal requirements and the National Data Classification Framework, ensuring Sensitive data is securely erased or destroyed when no longer needed. For Sensitive data, if backups involve storage outside Kuwait (such as cloud backups), obtain any required approvals in line with data sovereignty requirements.

8.6 PR–6 Physical Protection of Critical IT Assets

Control ID	Control Title	Purpose / Description	Minimum Requirement
PR–6	Physical Protection of Critical IT Assets	Reduce the risk of tampering, theft or damage to critical IT equipment.	Identify critical IT areas (for example, data centers, server rooms, main network rooms, and locations where backup media are stored) and keep a simple list of

			according to business need. Configure email domains with appropriate anti–spoofing controls (SPF, DKIM, DMARC) to prevent impersonation. Train staff to be cautious with unexpected links and attachments, and to report suspicious messages.
Control ID	Control Title	Purpose / Description	Minimum Requirement
PR–4.1	Approved Communication & Videoconferencing Platforms	Reduce risk from unapproved chat/voice/video tools and remote control apps.	For official work (meetings, calls, messaging, screen sharing), use only Entity–approved communication and collaboration platforms. Do not use personal or unapproved apps (for example, private messaging, personal email, unauthorized remote–control tools) for work data or meetings. Maintain a simple list of approved platforms and ensure staff are aware of it. Where feasible, restrict installation or use of unapproved tools on corporate devices via configuration.
Control ID	Control Title	Purpose / Description	Minimum Requirement
PR–4.2	Portable Media Device Control	Limit the risks from use of unapproved removable media devices.	Where feasible, restrict or technically disable the use of unapproved portable storage media (e. g., USB drives) on

			configuration changes), prioritizing Critical Systems and the central logging solution where used. • Retain logs for at least 90 days live and 12 months in total (live or archived). Review logs for suspicious activity at a frequency appropriate to the Entity's risk (for example, weekly for smaller Entities, daily for higher-risk environments).
DE-2	Time Synchronization	Ensure consistent timestamps across systems to facilitate incident investigation.	• Ensure all information systems (servers, workstations, network devices) synchronize their system clocks to a reliable, authoritative time source (e. g., NTP). Timestamps in logs MUST be consistent across the infrastructure. Periodically verify that system clocks remain in sync (for example, by comparing log timestamps from different systems).

10. RESPOND (RS) – Incident Reporting & Management

Control ID	Control Title	Purpose / Description	Minimum Requirement
RS-1	Incident Reporting to NCSC & Leadership	Ensure serious incidents are reported to NCSC and handled by designated leaders.	Establish and communicate a simple incident reporting process so that staff know how to report suspected incidents (for example, phishing, data loss, or system compromise). Appoint one person as the incident response lead and at least one backup to coordinate incident handling, even if external service

			them. For these areas, implement basic physical protections appropriate to the site, including at least: • Doors or cabinets that can be locked when the area is unattended. • Restricted access so that only authorized personnel can enter or unlock equipment (for example, keys, access cards, or codes managed by IT or facilities). • A simple record of non-routine visitors (such as contractors or vendors) to critical IT areas, which MAY be kept using existing building or guard logs. Store backup media and portable equipment (such as laptops) in a locked room or cabinet when not in use; avoid leaving them unattended in public or shared areas. This control focuses on the physical protection of IT assets and SHOULD make use of the entity's existing building or facility security arrangements wherever possible.

9. DETECT (DE) – Logging & Monitoring

Control ID	Control Title	Purpose / Description	Minimum Requirement
DE-1	Audit Logging & Monitoring	Provide visibility into suspicious activity and support investigations.	Enable audit logging on critical systems, network devices, security tools, and key applications. At minimum, log authentication events, administrative actions, and important security events. Where feasible, centralize logs into a basic logging solution for easier review. • Restrict access to logs to authorized personnel only and protect logs from unauthorized modification or deletion (including logging

Control ID	Control Title	Purpose / Description	Minimum Requirement
RC–1	Recovery Planning	Support structured recovery after incidents and disruptions.	Maintain a simple recovery plan or documented procedures for restoring critical systems and services after incidents or other disruptions. The plan SHOULD reference backup locations, key contacts, and any sequencing needed for restoration, especially for Sensitive and Restricted data. Review and update the plan at least annually and after major changes.
RC–2	Testing & Continuous Improvement	Ensure recovery works in practice and improvements are implemented.	Conduct basic recovery or continuity tests (for example, tabletop exercises or partial restoration tests) for critical systems at least annually. After tests or real incidents, capture lessons learned, update procedures and controls where practical, and track completion of agreed improvements.

12. Appendix A – Cloud Security Minimum Controls

This Appendix applies to all Entities using public cloud services, including Software–as–a–Service (SaaS), Platform–as–a–Service (PaaS), and Infrastructure–as–a–Service (IaaS). It complements the national baseline controls by addressing the unique characteristics of cloud computing.

In this Appendix, the Entity refers to the entity acting as the cloud tenant/customer, and CSP refers to the Cloud Service Provider.

Core Principles:

- Shared Responsibility: Security in the cloud is a partnership. The Cloud Service Provider (CSP) secures the infrastructure, while the Entity secures the data and configuration.
- Identity as the Perimeter: In the cloud, identity (who you are) is more critical than the network (where you are).

			providers are used. Maintain up–to–date contact details for the incident lead, backup, relevant service providers, and NCSC. Where an actual or suspected cybersecurity incident or threat may be reportable under NCSC–issued incident management or reporting guidance, the Entity MUST notify NCSC promptly through the official channels and within the applicable timelines set by NCSC. Where appropriate, the Entity MUST use out–of–band communication channels during active incidents or where normal channels may be affected. The Entity MUST provide follow–up updates and information as required by applicable NCSC reporting guidance.
RS–2	Basic Incident Handling & Coordination	Provide a structured but simple way to handle incidents and cooperate with NCSC.	Maintain a short written incident response procedure that covers: initial triage, containment, communication, evidence preservation, recovery, and reporting/escalation (including when and how to notify NCSC and other regulators or law enforcement). When NCSC or another competent authority notifies the entity of a potential incident, promptly triage and investigate, take reasonable remedial actions, and provide feedback where requested. After significant incidents, perform a brief lessons–learned review and record key improvements to be implemented, and share relevant lessons learned with NCSC or sector authorities where appropriate.

11. RECOVER (RC) – Recovery & Improvement

	Matrix	(IaaS, PaaS, or SaaS) and the resulting division of security responsibilities. The Entity retains accountability for Data Classification, Identity & Access Management (IAM), and Resource Configuration, regardless of the model.
CLD–8	Cloud Asset Inventory	Maintain a real–time inventory of cloud resources. Use programmatic resource tagging to identify the Data Classification (Public, Restricted, Sensitive) and Business Owner of each resource.

A.3 Identity & Access Management (IAM)

Control ID	Control Title	Minimum Requirement
CLD–9	MFA for Cloud Consoles	Multi–Factor Authentication (MFA) MUST be enforced for all users with administrative access to the Cloud Management Console and root accounts.
CLD–10	Service Account Hygiene	Service Accounts (non–human identities) MUST NOT be used for interactive human login. Keys for service accounts SHOULD be rotated periodically based on risk, or managed via automated identity federation (e.g., OIDC) to prevent credential theft.

A.4 Data Protection & Sovereignty

Control ID	Control Title	Minimum Requirement
CLD–11	Encryption by Default	All data at rest in the cloud MUST be encrypted. Entities SHOULD utilize the CSP's default encryption (platform–managed keys) as a minimum standard. For Sensitive data, Entities MAY opt for Customer–Managed Encryption Keys (CMEK) on cloud, based on a risk assessment. In accordance with Decision (1) of 2025.
CLD–12	Data Residency (Customer Content)	The Entity MUST configure cloud services and related contracts to store and process Customer Content (files, databases, application data) according to the National Data Classification Framework (Decision No. 1 of 2025).
CLD–13	Operational Metadata Exemption	Residency requirements apply to Customer Content. Operational Metadata (e.g., project IDs, billing

Crucial Distinction: Customer Content vs. Operational Metadata – To ensure the baseline is technically feasible, it is vital to distinguish between the Entity's data and the system data required to run the cloud. Customer Content: (Files, databases, application data). Residency and processing rules apply to Customer Content in accordance with the National Data Classification Framework and this Appendix. Operational Metadata: (Resource IDs, file names, IP addresses, billing logs, system status).

A.1 Cloud Acquisition & Contractual Governance

Goal: Ensure security is embedded before the contract is signed, leveraging existing national authorizations and global standards.

Control ID	Control Title	Minimum Requirement
CLD–1	Regulatory Authorization	Entities MUST ensure the Cloud Service Provider (CSP) is authorized to operate in the State of Kuwait in accordance with regulations issued by the relevant national authorities
CLD–2	Provider Due Diligence	Prior to selection, Entities MUST evaluate the CSP's security posture. This requirement is satisfied by reviewing the CSP's valid, independent international security certifications (e.g., ISO 27001, SOC 2 Type II, CSA STAR Level 2).
CLD–3	Right to Audit (Third–Party Assurance)	Contracts MUST include a "Right to Audit." To protect the security of multi–tenant environments, this right is exercised by the Entity reviewing the CSP's independent Third–Party Audit Reports (e.g., SOC 2, C5) rather than conducting physical data center visits.
CLD–4	Incident Notification Clause	Contracts MUST include a commitment from the CSP to notify the Entity of a confirmed data incident without undue delay to allow for accurate investigation and reporting.
CLD–5	Data Ownership & Exit	The contract MUST explicitly state that the Entity retains exclusive ownership of their data. The CSP MUST provide tools or standard APIs to allow the Entity to retrieve their data upon contract termination.
CLD–6	Service Level Agreements (SLAs)	Contracts MUST define Service Level Agreements (SLAs) for availability. The agreement SHOULD include financial remedies (service credits) for failure to meet these standards.

A.2 Governance & Shared Responsibility

Control ID	Control Title	Minimum Requirement
CLD–7	Shared Responsibility	Entities MUST document the cloud service model

Compensating Control	An alternative control that reduces risk to a comparable level when a Minimum Requirement cannot be met as written; it MUST be documented and approved as part of an exception.
Evidence	Documentation or artifacts demonstrating implementation (for example: policy, procedures, configurations, logs, tickets, inventories, or reports) sufficient for audit and oversight review.
Data classification levels	As defined in the National Data Classification Framework (Decision No. 1 of 2025).
Cloud Service Provider (CSP)	The provider of cloud services (for example: SaaS, PaaS, IaaS) used by the Entity.
Customer Content	Data provided to, created by, or managed for the Entity within cloud services (for example: files, databases, application data).
Operational Metadata	System and service metadata required to operate, secure, monitor, and bill cloud services (for example: resource IDs, billing logs, system status, IP addresses).

Unless explicitly defined in this document or in referenced national instruments, undefined technical terms should be interpreted using the NIST glossary. In case of any discrepancy, definitions in applicable national instruments and NCSC issuances take precedence.

B.2 Acronyms

Acronym	Meaning
CIS	Center for Internet Security
CMEK	Customer-Managed Encryption Keys
CSA	Cloud Security Alliance
CSA CCM	Cloud Controls Matrix
CSP	Cloud Service Provider
CSF	Cybersecurity Framework
DE	Detect (NIST CSF function)
EDR	Endpoint Detection and Response
GOV	Govern (NIST CSF function)
IAM	Identity and Access Management
ID	Identify (NIST CSF function)
IG1	Implementation Group 1
IaaS	Infrastructure as a Service
MFA	Multi-Factor Authentication
NCSC	National Cyber Security Center
NDA	Non-Disclosure Agreement
NIST	National Institute of Standards and Technology
PaaS	Platform as a Service
PR	Protect (NIST CSF function)
RC	Recover (NIST CSF function)
RS	Respond (NIST CSF function)
SaaS	Software as a Service
SIEM	Security Information and Event Management
SLA	Service Level Agreement
SPF	Sender Policy Framework
DKIM	DomainKeys Identified Mail
DMARC	Domain-based Message Authentication, Reporting, and Conformance

		logs, system status, and IP addresses) can be processed globally to ensure platform security, reliability, and accurate billing. Entities must ensure that metadata identifiers (such as Project IDs, folder names and labels) remain non-sensitive.
CLD-14	Public Access Prevention	Cloud storage resources (e. g., object storage buckets) MUST be configured to block public access by default. Public exposure MUST be an explicit, documented exception approved by the data owner.

A.5 Operational Security

Control ID	Control Title	Minimum Requirement
CLD-15	Cloud Audit Logging	Enable audit logging for cloud projects. Logs MUST capture "Admin Activity" (configuration changes) and "Data Access" (who accessed data) for sensitive workloads. Retain logs for a minimum of 12 months.
CLD-16	Secure Connectivity	All traffic between the entity and the cloud provider MUST be encrypted in transit using industry-standard protocols (e. g., TLS 1.2 or higher). Management interfaces MUST NOT be exposed directly to the public internet; use secure bastions, VPNs, or Identity-Aware Proxies.

13. Appendix B – Glossary and Acronyms

B.1 Glossary

Term	Definition
Entity	Civil, military, or security government agencies, as well as public and private sector agencies within the State of Kuwait that are relevant to the Center, and other entities designated by the chief of NCSC in accordance with the provisions of Amiri Decree No. 37 of 2022.
Minimum Requirements	The mandatory control statements in this baseline. Guidance and implementation notes are non-mandatory unless explicitly stated as a requirement.
Applicable	A requirement that is relevant to the Entity's environment, systems, and services and is therefore included in compliance calculation.
Not Applicable (N/A)	A requirement that does not apply to the Entity's environment, with documented justification and approval per the Entity's governance process.
Exception	A formally approved, time-bound deviation from a Minimum Requirement, documented under the exception process (GOV-2), including scope, duration, and compensating controls where applicable.