QATAR NATIONAL INFORMATION ASSURANCE

National ICS Security Standard

[January 2013]

Version: **2.0**

Classification: **Public - Final**

Appendix A is normative parts of this standard. Appendix B is informative only.

TABLE OF CONTENTS

1. INTRODUCTION

Critical Infrastructure organizations that depend on Industrial Control Systems (ICS) have begun using commercial-off-the-shelf (COTS) technology developed for business systems in their everyday processes. This has provided an increased opportunity for cyber attacks against the critical systems they operate. These COTS systems are not usually as robust (at dealing with cyber attacks) as are systems designed specifically for Critical Infrastructure at dealing with cyber attack for many reasons. These weaknesses may lead to health, safety and environmental (HSE), or operational consequences that could severely impact the State of Qatar's economy, people or Government.

This ICS security baseline standard document provides the minimum controls that need to be incorporated or addressed for any ICS system that has been determined to be critical to the State of Qatar. This document is to be used together with a suitable risk based security management program.

1.1. Scope

When assessing assets of a critical ICS system the following should be included:

- Control centres and backup control centres including systems at master and remote sites
- Transmission substations that support the reliable operation of the bulk systems
- Systems and facilities critical to system restoration, including black start generators and substations in the electrical path of transmission lines used for initial system restoration
- Systems that provide monitoring, control, automatic generation control, real time systems modelling, and real time inter-utility data exchange.

2. ICS SECURITY POLICY

2.1. Policy Objective

The objective of this policy is to provide management direction, approval and support for ICS security in accordance with business requirements and relevant laws and regulations.

2.2. Policy & Baseline Controls

2.2.1. ICS security policy document	An ICS security policy document SHALL be approved by senior management, and published and communicated to all employees and relevant external parties either as part of the organization's information security policy or as a separate policy.
2.2.2. Security program leadership	The senior management responsible for ICS security SHALL be identified by name, title, business phone, business address and date of designation. Changes to the senior management MUST be documented within thirty (30) calendar days of the effective date.
2.2.3. Review of the security policy	The security policy SHALL be reviewed annually or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness.

3. ICS PROCUREMENT PROCESS

3.1. Policy Objective

The objective of this policy is to ensure security principles are considered when procuring control systems products (software, systems, services and networks).

3.2. Policy & Baseline Controls

3.2.1. Procurement language and process	The Procurement Language and Request for Proposal (RFP) SHALL follow the guidelines in Appendix B.
3.2.2. System acceptance	Acceptance criteria for new ICS systems, upgrades, and new versions SHALL be established in accordance to the approved ICS policy document and suitable tests of the system(s) carried out during development and prior to acceptance. All acquired systems SHALL comply with the controls in this document.
3.2.3. Outsourcing contracts	The security requirements of an organization outsourcing the management and/or control of all /some of its ICS systems, networks and desktop environment SHALL be addressed in a contract agreed between the parties. The organisation SHALL ensure that the baseline controls specified in this Document are included in the third party service delivery agreement or contract. This SHALL also apply to sub-contractors used by the third party.

4. ORGANIZATIONAL SECURITY

4.1. Policy Objective

The objective of this policy is to have a well-defined organisational security when managing ICS systems.

4.2. Policy & Baseline Controls

4.2.1. Incorporating ICS security	Management SHALL incorporate the management of ICS security within the organizational governance/ security scheme or security program and explicitly acknowledge their ICS security responsibilities.
4.2.2. ICS change management	The organization SHALL establish a dedicated ICS change management committee that reviews and approves proposed changes. This committee SHALL have representation from corporate IT amongst other as necessary.
4.2.3. ICS security coordination	ICS security activities SHALL be coordinated by representatives from different parts of the organization with relevant roles and job functions, e.g. Physical security, Emergency Response, Corporate IT, etc.
4.2.4. Allocation of ICS responsibilities	All ICS responsibilities SHALL be clearly defined.
4.2.5. Authorization process for ICS information processing facilities	A management authorization process for new ICS information processing facilities SHALL be defined and implemented.
4.2.6. ICS Confidentiality agreements	Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of the ICS Information SHALL be identified and regularly reviewed.
4.2.7. Establishing Contact with authorities	Appropriate contacts with relevant authorities SHALL be maintained, including the National CERT (Q-CERT) and emergency services.
4.2.8. Contact with special interest groups	Appropriate contacts with special interest groups or other ICS specialist security forums (e.g. Qatar's EN-IREC) and professional associations SHALL be maintained.

5. PHYSICAL AND ENVIRONMENTAL SECURITY

5.1. Policy Objective

The objective of this policy is to prevent unauthorized physical access, damage and interference to the ICS premises, equipment and information.

5.2. Policy & Baseline Controls

5.2.1. Physical security perimeter	Dedicated security perimeters (e.g. barriers such as walls, card controlled entry gates, CCTVs or manned reception desks) SHALL be used to protect areas that contains ICS processing facilities.
5.2.2. Communication medium	Extra/separate physical protections SHALL be in place to protect the ICS distribution/communication lines from accidental damage, tampering, eavesdropping or in transit modification of unencrypted communications. Protective measures include: locked wiring closets/ manholes, protected cabling duct or trays, etc.
5.2.3. Display Medium	Controls for the physical access to devices that display ICS information SHALL be in place. See 5.2.1.
5.2.4. Portable and mobile devices security within the control rooms	The organization SHALL establish controls against the usage of mobile and portable devices within the control rooms and restrict them (as a default) unless they are explicitly authorised or pre-approved and they are owned and audited by the organisation.

6. COMMUNICATION AND OPERATIONS MANAGEMENT

6.1. Policy Objective

The objective of this policy is to ensure the correct and secure operation of ICS information processing facilities.

6.2. Policy & Baseline Controls - Operational Procedures and Responsibilities

6.2.1. Documented operating procedures	ICS operating procedures SHALL be documented, maintained, and made available to all authorized users who need them. Vendors SHALL supply the organization with the full documentation for any operating procedure required on their systems.
6.2.2. Change management	Changes to ICS information processing facilities and systems SHALL be controlled and pre-approved by the dedicated ICS change management committee. See 4.2.2.
6.2.3. Separation of development test and operational facilities	Development, test and operational facilities SHALL be physically separated to reduce the risks of unauthorized or inadvertent access or changes to operational systems.

6.3. Policy & Baseline Controls - Third Party Service Delivery Management

6.3.1. Service delivery	Organisations SHALL ensure that the security controls, service definitions and delivery levels included in third party service delivery agreement are implemented, operated, and maintained by the third party.
6.3.2. Monitoring and review of third party services	The services, reports and records provided by the third party SHALL be regularly monitored and reviewed, and audits SHALL be carried out regularly.
6.3.3. Managing changes to third party services	Changes to the provision of services, including maintaining and improving existing ICS security policies, procedures and controls, SHALL be managed, taking account of the criticality of systems and processes involved and re-assessment of consequent risks.

6.4. Policy & Baseline Controls - Patching and the Protection against Malicious and Mobile Code

6.4.1. Controls against malicious code	Detection, prevention, and recovery controls to protect against malicious code and appropriate user awareness procedures SHALL be implemented and documented. These controls include installing anti-malware software, and "whenever technically possible" using white lists of pre-approved processes, etc.
6.4.2. Anti-malware deployments	The ICS Anti-malware solution SHALL be regularly updated with the ICS vendor latest published and approved malware definitions or signatures; It's also highly RECOMMENDED that the organization utilizes a different Anti-malware product that the one used on the corporate LAN.
6.4.3. Controls against mobile code	Where the use of mobile code[1] is authorized, the configuration SHALL ensure that the authorized mobile code operates according to a clearly defined security policy, and unauthorized mobile code SHALL be prevented from executing.
6.4.4. Patch Management	The responsible entity, either separately or as a component of the documented configuration management process, SHALL establish and document a security patch management program for tracking, evaluating, testing and installing applicable software patches for ALL the system assets (Including network components) in a timely manner as per the following: ▸ The responsible entity SHALL document the assessment of security patches and upgrades for applicability within fifteen (15) calendar days of availability of the patch or upgrade from the vendor ▸ The responsible entity SHALL document the implementation of security patches. In any case where the patch is not installed, the responsible entity SHALL document compensating measure(s) applied to mitigate risk exposure or an acceptance of risk ▸ Internal procedures for applying critical/urgent patches or compensating controls SHALL be developed in case the vendor can not deploy critical patches in a timely manner
6.4.5. Technical vulnerabilities	Timely information about technical vulnerabilities (Including Zero day Vulnerabilities) of information systems being used SHALL be obtained, the organization's exposure to such vulnerabilities evaluated, and appropriate measures taken to address the associated risk.

[1] Scripts like JavaScript and VBScript, Java applets, ActiveX controls and macros embedded within office documents, etc.

6.5. Policy & Baseline Controls – Backup

6.5.1. Information backup	Back-up copies of ICS information and software SHALL be taken and restoration tested regularly (At least Annually) in accordance with an agreed backup policy.
6.5.2. Offsite backups	At a minimum, full monthly backups SHALL be stored offsite at a secure facility with full documentation for the offsite backup handling process. Backups MUST be encrypted if there are to be stored at a third party or outside the jurisdiction of the State of Qatar.
6.5.3. Equipment replacement and spare parts	The organization SHALL ensure the availability of critical equipment backup components and spare parts.

6.6. Policy & Baseline Controls – Network Security and its Management

6.6.1. Network controls	Networks SHALL be adequately managed and controlled, in order to be protected from threats, and to maintain security for the systems and applications using the ICS network, including information in transit.
6.6.2. Security of networks services	Security features, service levels, and management requirements of all network services SHALL be identified and included in any network services agreement, whether these services are provided in-house or outsourced.
6.6.3. ICS Network architecture	Organisations SHALL utilize a three-tier network architecture (as a minimum) which include each of the following components in a physically/logically separate tier: ▸ Corporate/Enterprise LAN ▸ ICS Shared DMZ ▸ ICS network ▸ The architecture avoids single point of failures by means of equipment high availability, redundancy and alternate passes A stateful firewall SHALL be deployed between each of the above layers.
6.6.4. No direct connections from the Internet to the ICS network and vice versa	Internet connections SHALL NOT terminate directly into the ICS network; In case of a time limited, continuously monitored and approved exception a firewall SHALL be used to isolate the ICS network from the Internet
6.6.5. Restricted access from the corporate network to the control network	Firewalls SHALL be used to segregate corporate networks from control networks. The firewall base rule SHALL be "*deny all, allow explicitly*". Inbound connections to the ICS networks SHALL be limited. In exceptional cases where inbound connections are absolutely necessary, management sign-off on this risk SHALL be obtained. Outbound traffic through the ICS firewall SHALL be limited to essential communications only. All outbound traffic from the ICS to the corporate network SHALL be source and destination restricted by service and port using static firewall rules.
6.6.6. Intrusion detection and prevention	An IDS/IPS solution SHALL be implemented at the ICS DMZ level to detect possible intrusions from the Corporate network, it's Also RECOMMENDED that the organization deploys IDS/IPS within the ICS network if technically supported.

6.6.7. Secure methods for authorized remote support of control systems	Management or support traffic SHALL be via a separate, secured management network or over an encrypted network/tunnel (Such as VPN) with three-factor authentication for connections from the corporate LAN or 3rd party networks. Traffic SHALL, additionally, be restricted by IP address to specific management/support stations. Logs generated from remote connections SHALL be kept for a period of not less than 90 days. As per section 6.9
6.6.8. Secure connectivity for wireless devices	Wireless devices SHOULD be avoided in critical ICS systems. Where this is not possible, the organization SHALL use authentication and cryptography for enhanced security mechanisms (at least utilizing WPA encryption for 802.11x networks) to prevent unauthorized wireless access into the ICS system. It's RECOMMENDED to adopt the ISA100a standard for wireless connectivity whenever possible. The wireless technologies include, but are not limited to microwave, satellite, packet radio [UHF/VHF] and 802.11x.
6.6.9. Well defined rules outlining the type of traffic permitted on a network	The allowed types (protocol/ports) of the traffic SHALL be defined, approved and documented.
6.6.10. Monitoring and logging of ICS network traffic	Organisations SHALL "continuously" monitor and retain the ICS network logs for a period of not less than 90 days. And It's highly RECOMMENDED that all the logs are centrally stored and managed. As per section 6.9
6.6.11. Industrial Protocols (MODBUS/TCP, EtherNet/IP and DNP3)	ICS related protocols such as (MODBUS/TCP, EtherNet/IP and DNP3) SHALL only be allowed within the ICS networks and not allowed to cross into the corporate network.
6.6.12. ZigBee wireless communication	The ZigBee network SHALL meet the following: - Network Infrastructure is protected with a network key - Encryption security service is enabled - Filtering done via MAC addresses - Source node authentication enabled
6.6.13. Data Historians and related services	A three-zone design SHALL be adopted when implanting data historians where the organization utilizes a two server model. One data historian server is placed on the ICS network to collect the data from the control / RTUs and a second server on the corporate network mirroring the first server and supporting client queries.

6.6.14. Dial-Up Modems	Organisation SHALL limit the use of dial-up modems connected to the ICS networks. Where other alternatives are not possible, the following controls SHALL be in place: ▸ Call back features ▸ Default passwords SHALL be changed ▸ Physically identify the modems in use to the control room operators. And make sure they are counted and registered in the approved HW inventory ▸ Disconnect the modems when not in use or setup them up to automatically disconnect after being idle for a given period of times ▸ If modems are used for remote support, make sure these guidelines are well communicated to the support personnel.
6.6.15. Equipment identification in networks	Automatic equipment identification solutions SHALL be used as a means to authenticate connections from specific locations and equipment. And to detect rouge connections and devices.
6.6.16. Remote diagnostic and configuration port protection	Physical and logical access to diagnostic and configuration ports (on ICS systems, field devices, sensors, antennas and communication devices) SHALL be controlled.
6.6.17. Segregation of networks	Information services, users, and information systems SHALL be segregated on networks.
6.6.18. Segregation of duties	Segregation of duties for ICS security operating personnel SHALL be followed.
6.6.19. Network connection control	For shared networks, especially those extending across the organization physical boundaries, the capability of users to connect to the ICS network SHALL be denied. Named exceptions SHALL be in line with the access control policy.
6.6.20. Data Diodes	It's RECOMMENDED to utilize the Data Diode technologies for additional security whenever only one-way communication is required.
6.6.21. ICS Firewall deployments	It's highly RECOMMENDED that the organization utilizes a different Firewall product than the one used on the corporate LAN.

6.7. Policy & Baseline Controls – Media Handling

6.7.1. Management of removable media	Removable media (such as USB/CD/DVD) SHALL NOT be allowed into the ICS control room or used within the system unless explicitly authorized by management. The removable media ports/drivers SHALL be blocked by default.
6.7.2. Disposal of media	Media SHALL be disposed when no longer required, using the organization's formal procedures for safe and secure information sensitization.
6.7.3. Information handling procedures	Procedures for the handling and storage of ICS information SHALL be established to protect this information from unauthorized disclosure or misuse.
6.7.4. Security of system documentation	ICS System documentation SHALL be protected against unauthorized access or unauthorized disclosure.

6.8. Policy & Baseline Controls – Exchange of ICS Information

6.8.1. Information exchange policies and procedures	Formal exchange policies, procedures, and controls SHALL be in place to protect the exchange of information through the use of all types of communication facilities (emails, Faxes, PSTN, GSM…etc)
6.8.2. Exchange agreements	Special Agreements SHALL be established for the exchange of ICS information and software between the organization and external parties.
6.8.3. Physical media in transit	Media containing ICS information SHALL be protected against unauthorized access (e.g. by using encryption), misuse or corruption during transportation beyond an organization's physical boundaries. Details of acceptable encryption protocols/keys are specified in Appendix A.
6.8.4. Electronic messaging	ICS information sent via electronic messaging SHALL be appropriately protected.

6.9. Policy & Baseline Controls – Monitoring

6.9.1. Audit logging	Audit logs, recording user activities, exceptions, and information security events, SHALL be produced and kept for ninety (90) calendar days to assist in access control/authorisation monitoring and to support any investigations.
6.9.2. Central Logging	It's RECOMMENDED that logs are kept and managed centrally on a dedicated logging infrastructure.
6.9.3. Monitoring system use	Procedures for regularly monitoring use of ICS information processing facilities SHALL be established and the results of the monitoring activities reviewed regularly.
6.9.4. Protection of log information	Logging facilities and log information SHALL be protected against tampering and unauthorized access. ICS logs SHALL be stored both physically and logically separate from corporate IT logs.
6.9.5. Administrator and operators logs	ICS administrators' and operators' activities SHALL be logged.
6.9.6. Fault logging	Faults SHALL be logged, analyzed, and appropriate action taken.
6.9.7. Clock synchronization	The clocks of all relevant ICS systems within an organization SHALL be synchronized with an accurate (UTC or GMT+3) time source.

7. ACCESS CONTROL

7.1. Policy Objective

The objective of this policy is to control access to ICS systems and information and ensure the availability of ICS access control logs and functionality of the overall process.

7.2. Policy & Baseline Controls – Access Policy and User Access Management

7.2.1. Access control policy	An ICS access control policy SHALL be established, documented, and reviewed based on business and security requirements for granting access. The policy SHALL be based on the *least privilege* and *personal/named accountability* concepts. Account management may include additional account types (e.g., role-based, device-based, attribute-based).
7.2.2. User registration	There SHALL be a formal ICS user registration and de-registration procedure in place for granting and revoking access to all related systems and services. This procedure SHALL be communicated to the corporate IT and Personnel (HR) departments.
7.2.3. Privilege management	The allocation and use of privileges SHALL be restricted and controlled. The responsible entity SHALL ensure that individual and shared accounts are consistent with the concept of *need to know/need to share* with respect to work functions performed.
7.2.4. User password management	The allocation of passwords SHALL be controlled through a formal management process.
7.2.5. Password complexity	The organisation SHALL require and use passwords subject to the following (as technically feasible): ▸ Each password/pass phrase SHALL be a minimum of twelve characters ▸ Each password SHALL be changed at least annually, or more frequently based on the adopted risk assessment.
7.2.6. Review of user access rights	Management SHALL review user access rights at regular intervals using a formal process. Security personnel who administer access control functions SHALL NOT administer the review/audit functions.
7.2.7. Testing	The responsible entity SHALL implement a maintenance and testing program to ensure that all security functions under the "Access Control" section function properly

7.3. Policy & Baseline Controls – Network and Operating System Access Control

7.3.1. Policy on use of ICS network services	Users SHALL only be provided with access to the ICS services that they have been specifically authorized to use.
7.3.2. Secure log-on procedure	Access to ICS systems SHALL be controlled by a secure log-on procedure inline with the organisation's access control policy.
7.3.3. User identification and authentication	All users or processes "acting on behalf of users" SHALL have a unique identifier (user ID) for their sole and intended use only, and a suitable authentication technique SHALL be chosen to substantiate the claimed identity of the user/process. Expect where it is technically impossible to utilize a personal/named identification[2], the following SHALL be maintained: ▸ A recorded valid need-to-know/need-to-share that is determined by assigned official duties and satisfying all personnel security criteria ▸ Compensating controls for automated user identification such as CCTV, Smart cards…etc. ▸ The organization specifically authorizes and monitors the use of guest/shared/anonymous accounts and removes, disables, or otherwise secures unnecessary accounts. ▸ The organization removes, changes, disables, or otherwise secures default accounts. ▸ Account/shift managers are notified when users are terminated or transferred and associated accounts are removed, disabled, or otherwise secured. ▸ Account/shift managers are also notified when users usage or need-to-know/need-to-share changes. ▸ In cases where accounts are role-based, i.e., the workstation, hardware, and/or field devices define a user role, access to the ICS SHALL include appropriate physical security controls, which can identify the operator and record time of entry/departure.

[2] Identifier management is not applicable to shared ICS accounts. Where users function as a single group (e.g. control room operators in legacy systems), user identification may be role-based, group-based, or device-based. For some systems, the capability for immediate operator interaction is critical. Local emergency actions for the ICS MUST not be hampered by identification requirements. Access to these systems may be controlled by appropriate physical security mechanisms or other compensating controls.

7.3.4. Password management systems	Systems for managing/storing ICS passwords SHALL be interactive and SHALL ensure quality passwords.
7.3.5. Use of system utilities	The use of utility programs that might be capable of overriding system and application controls SHALL be restricted and tightly controlled.
7.3.6. Session time-out	Inactive ICS sessions SHALL shut down automatically after a defined period of inactivity.
7.3.7. Concurrent session control	ICS systems SHALL limit the number of concurrent sessions for any given user and/or username inline with the organisation's policy on concurrent sessions.
7.3.8. Limitation of connection time	Restrictions on connection times SHALL be used to provide additional security for high-risk applications.

7.4. Policy & Baseline Controls – Field Device Access & Remote Terminal Units (RTUs)

7.4.1. Dial UP RTUs that doesn't have routable protocols	Devices such as Remote Terminal Units (RTUs) that do not use routable protocols are not required to be enclosed in the physical security perimeter, but SHALL be enclosed and monitored within the electronic security perimeter.
7.4.2. Dial up RTUs that have routable protocols	Devices such as RTUs that use routable protocols SHALL be enclosed within the entity's physical security perimeter as well as the electronic security perimeter.
7.4.3. Authenticating RTUs	It is RECOMMENDED that secured field devices use cryptographic certificates issued/trusted by a plant certificate authority to ensure device identity.
7.4.4. Direct access to operational field device	Any direct access to operational field devices that is made by field personnel SHOULD be provided in such a way that there are permission checks applied to that access; there is personal accountability (e.g., record keeping with human identity) for any action via that access; and the resulting device state remains consistent with any copies of that state that are cached by the control system.
7.4.5. RTUs access logging	Secured field devices SHOULD provide the capability to detect and discard received messages whose reception timing, relative to the expected moment of their transmission, or whose sequence violates the quality of service characteristics of the communications session.
7.4.6. RTU Communication interface	Communication links to RTUs SHOULD be encrypted as specified in Appendix A. Encryption implemented on the communication interface SHOULD NOT degrade the functional or performance capability of the operational function that has the authorization to access the RTU.

8. INFORMATION SECURITY INCIDENT MANAGEMENT

8.1. Policy Objective

The objective of this policy is to ensure information security events and weaknesses associated with ICS information systems are communicated in a manner allowing timely corrective action to be taken.

8.2. Policy & Baseline Controls

8.2.1. ICS Incident response plan	The responsible entity SHALL develop and maintain an ICS information security incident response plan to address at a minimum, the following: ▸ Procedures to characterize and classify events as reportable security incidents ▸ Procedures to properly and in a timely manner report security incidents to the appropriate management channels ▸ Process for updating the incident response plan within thirty (30) calendar days for any changes in the reporting mechanism, organizational hierarchy, contacts, etc. ▸ Procedures to test the incidents response plan, at least annually. Tests can range from table top drills to full operational exercise scenarios to the response to an actual incident.
8.2.2. Reporting security weaknesses	All employees, contractors and third party users of information systems and services SHALL note and report any observed or suspected security weaknesses in systems or services. This can be achieved by formally including the requirement in their contracts, job descriptions, etc...
8.2.3. Contacting the authorities	The responsible entity SHALL establish communication contacts as applicable with the national CERT (Q-CERT) for reporting incidents of criticality level one (as identified in the GIA/NIA Appendix C).

9. BUSINESS CONTINUITY MANAGEMENT

9.1. Policy Objective

The objective of this policy is to counteract interruptions to business activities and to protect critical ICS processes from the effects of major failures of information systems, network disruptions or disasters and to ensure their timely resumption.

9.2. Policy & Baseline Controls

9.2.1. ICS Business Continuity (BC) & Disaster Recovery (DR) Plan	The ICS Business Continuity Plan (BCP) SHALL be a component within the corporate BCP and SHALL include the following items as a minimum: ▸ Business impact classification and prioritization of the ICS assets ▸ Required response to events that would activate the plan ▸ Procedures for operating the systems' basic functionalities in a manual mode, until normal operational conditions are restored ▸ Roles and responsibilities of the ICS BCP responders ▸ Complete up to date documentation (manuals, configurations, procedures, vendors contact lists, network diagrams...etc) ▸ Personnel list for authorized physical and logical access to the systems ▸ System components restoration order/sequence ▸ Offsite backups recall and restoration procedures ▸ Procedures for liaison with the appropriate authorities as per the organization's BCP.

10. COMPLIANCE

10.1. Policy Objective

The objective of this policy is to avoid breaches of any law, statutory, regulatory or contractual obligations and to ensure compliance of systems with national and/or organizational security current or future policies and standards. It also covers system audit considerations.

10.2. Policy & Baseline Controls – Compliance

10.2.1. Identification of applicable legislation	All relevant statutory, regulatory and contractual requirements and the organization's approach to meet these requirements SHALL be explicitly defined, documented, and kept up to date for each information system and the organization.
10.2.2. Compliance with security policies and standards	Managers SHALL ensure that all security procedures within their area of responsibility are carried out correctly to achieve compliance with security policies and standards including this document.
10.2.3. Technical compliance In-house checking	ICS systems SHALL be regularly self-checked for compliance with security implementation standards, or guidelines including this document, at least annually.
10.2.4. Compliance Monitor and audit data retention	The auditee SHALL keep the last audit report and all the related documents for at least two years from the date the report was received.
10.2.5. Levels of non-compliance	Audit findings require rectification inline with the following schedule: ▸ Level 1: minor non-conformities and observations SHALL be rectified within six (6) months ▸ Level 2: major non-conformities SHALL be rectified within three (3) months.

10.3. Policy & Baseline Controls – System Audit

10.3.1. Information systems audit controls	Audit requirements and activities involving checks on ICS operational systems SHALL be carefully planned and agreed to minimize the risk of disruptions to business operations.
10.3.2. Protection of information systems audit tools	Access to ICS information systems audit tools SHALL be protected to prevent any possible misuse or compromise.

11. SYSTEM HARDENING

11.1. Policy Objective

The objective of this policy is to ensure unused services in a host operating system (OS)/ICS system are disabled. Only services used by the ICS system, its operation and maintenance should be enabled to limit possible entry points or vulnerabilities.

11.2. Policy & Baseline Controls

11.2.1. Vendor application white list	Organisations SHALL obtain and maintain a list of all applications, utilities, system services, scripts and all other software required to keep the ICS system operational.
11.2.2. Software/services to be removed	All unnecessary software/services SHALL be removed; this includes but not limited to: ▸ Games ▸ Device drivers for hardware not included ▸ Messaging services ▸ Servers or clients for unused internet or remote access services ▸ Software compilers (except from non-production, development machines) ▸ Software compliers for unused languages ▸ Unused protocols and services ▸ Unused administrative utilities, diagnostics, network management and system management functions ▸ Test and sample programs or scripts ▸ Unused productivity suites and word processing utilities for example: Microsoft word, excel, PowerPoint, adobe acrobat, open office, etc. ▸ Unlicensed tools and sharewares ▸ Universal Plug and Play services.
11.2.3. Restricting Bluetooth access	Bluetooth wireless access technology SHALL be denied by default.
11.2.4. BIOS Protection	The BIOS (Basic Input/Output System) SHALL be password protected from unauthorized changes.
11.2.5. Disabling well known or Guest accounts	Default accounts and passwords SHALL be disabled or changed to meet the organization complexity requirements.
11.2.6. Equipment certification	It's highly RECOMMENDED that the ICS security devices utilized have achieved EAL (Evaluation assurance level) of 4+ as per the common criteria (ISO 15408).

APPENDIX A (NORMATIVE) – APPROVED CRYPTOGRAPHIC ALGORITHMS AND PROTOCOLS

Symmetric Key/Private Key:

Cryptographic functions that use a symmetric key cipher (sometimes referred to as private key encryption) employing a shared secret key must adopt any of the following specifications.

Algorithm Name	References	Approved Use	Required Key Length
AES	Advanced Encryption Standard block cipher based on the "Rijndael" algorithm [AES]	General Data Encryption	256-bit keys
TDES /3DES	Triple Data Encryption Standard (or Triple DES) block cipher [SP800-67]	General Data Encryption	three unique 56-bit keys
Note: AES SHOULD be used unless this is not technically possible. TDES usage should be limited to systems not supporting AES.			

Asymmetric Key/Public Key:

Cryptographic functions that use *asymmetric key ciphers* (also known as public key encryption) that employ a pair of cryptographic keys consisting of one public key and one private key must adhere to the following specifications:

Algorithm Name	References	Approved Use	Required Key Length
RSA	"Rivest-Shamir-Adleman" algorithm for public-key cryptography [RSA]	Digital Signatures, Transport of encryption session keys	1024-bit keys
DSA	Digital Signature Algorithm [FIP186-2]	Digital Signatures	1024-bit keys

Hashing algorithms

Secure hash algorithms can be used to support implementation of keyed-hash message authentication Generally, Hash functions are used to speed up data comparison tasks — such as finding items in a database, detecting duplicated or similar records in a large file or system.

Algorithm Name	References	Approved Use	Required Key Length
SHA-n	A secure hash algorithm that produces a hash size of "n" e.g.: (SHA 224, 256 ,384,512) [SHA]	All hashing purposes	n ≥ 256

MD5	Message Digest v5 [RFC 1321]	All hashing purposes	The typical 128-bit state
Note: SHAn SHOULD be used unless this is not technically possible. MD5 usage should be limited to systems not supporting SHA family.			

APPENDIX B (INFORMATIVE) – REFERENCE TO PROCUREMENT GUIDELINES

The RFP issued to ICS vendors should include the security requirements of the standard for the applicable domains such as:

- Network architecture security
- Removal of unnecessary services and programs
- Antimalware and host based intrusion protection and prevention
- Filesystem and O.S hardening
- Patching mechanisms including 3rd party patching
- Firewalls/IPS/IDS implementations
- Changing default accounts and role based access
- Password management
- Logging infrastructure
- Backup and restore procedures.

More supporting information can be found in the (Cyber Security Procurement Language for Control Systems) issued by ICS-CERT, 2009.

- http://ics-cert.us-cert.gov/pdf/FINAL-Procurement_Language_Rev4_100809.pdf

Where it further defines the following:

Topic Basis: A topic's basis is a summary of the potential exposures and vulnerabilities associated with a particular class of problem, that is, why the topic is included.

Procurement Language: Terminology as explained in section (14) of the document (Cyber Security Procurement Language for Control Systems).

Factory Acceptance Test Measures: The Factory Acceptance Test (**FAT**) is necessary to ensure security features function properly and provide the expected levels of functionality. Each topic in the RFP should include factory acceptance test tasks specific to that topic. Note that FAT is a process, not an event, and could in fact extend over several weeks or months.

Site Acceptance Test Measures: The ICS asset owner's Site Acceptance Test (**SAT**) typically repeats a subset of a FAT after system installation, but before cutover or commissioning, to demonstrate that the site installation is equivalent to the system tested at the Vendor's factory or as described in the Systems Manuals. Like the FAT, the SAT may extend several weeks or months and in addition occur at multiple locations.

Maintenance Guidance: This is guidance on how the vendor will maintain the level of system security established during the SAT as the system evolves, is upgraded, and patched. This subsection may be best included as a security clause in a maintenance contract, rather than in a procurement specification to maintain on-going support.

REFERENCES

The controls and knowledge in this standard are derived from the below sources:

- Q-CERT / CIIP Knowledge base (www.qcert.org)
- The Qatari EN-IREC (Energy sector- Information Risk Experts Committee)
- Qatar's NIA (National Information Assurance framework)
- ISA99/IEC 62443 (www.isa99.org)
- NERC (www.nerc.com)
- ISO27k (www.iso.org).