Book 8
Technical Specification and Requirements of Cyber Security

Table of Content

Technical Specification and Requirements of Cyber Security for Microgrid Development Project at Betong District Provincial Electricity Authority (PEA)

1. Introduction

This Technical Specification presents the technical and requirement of cyber security in the bidding document of Microgrid Development Project at Betong District, Yala. A microgrid benefits from a control or automation system that helps facilitate, automate, and optimize operation of the power system. However, microgrid also creates new vulnerabilities. The sophisticated distributed control of generation and demand opens up the possibilities for breaches of security. It is crucial that the control system operating a microgrid be secure against adversarial attack. Therefore cyber security will be essential element to be considered in this project, in order to meet the requirements with Distribution Dispatching Center Improvement Project (DDIP) which is ongoing project by PEA now. This document specifies the necessary details of requirement of cyber security of MGBT.

2. Principal Requirement

Microgrids are increasingly utilizing ICTs in the process of energy generation, delivery, and consumption within their territories. Accordingly, microgrid operations integrate the physical process with the computation, communication, and control functionalities that are realized by a cyber system. The microgrid cyber system is typically composed of a control center, a multitude of sensors and actuators embedded in dispersed field devices, and the associated communication infrastructure. Figure 1 presents the typical microgrid architecture from the cyber–physical perspective [1].

The control center normally comprises an application server, a historian, together with a human–machine inter-face (HMI). The historian is a database that logs the process information of microgrid operations, while the HMI provides an interface for visualizing real-time or historical operating conditions, and configuring operational functionalities. The application server is equipped with the supervisory control and data acquisition (SCADA) system and the energy management system (EMS). The EMS works in concert with the SCADA system. The SCADA system acts as the front–end interface to interact with field devices, whereas the EMS is the back–end processor with decision-making capabilities.

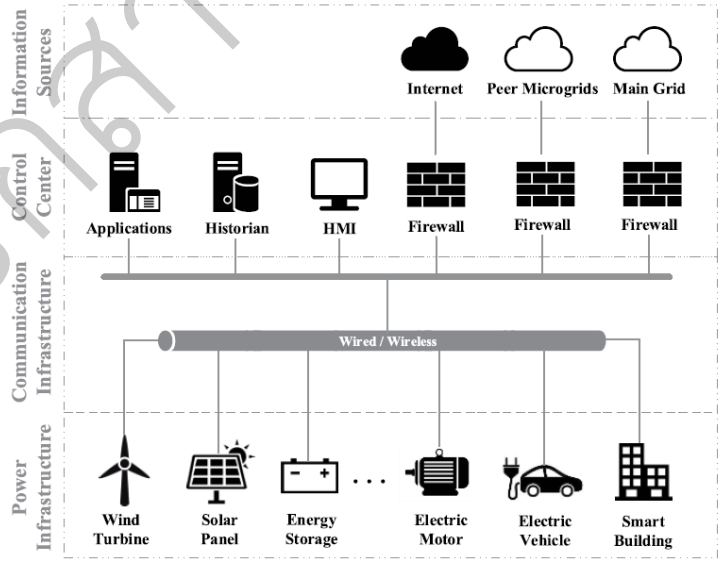

Figure 1: Typical microgrid architecture [1]

The communication network may be a heterogeneous amalgamation of wired systems such as fiber-optics and cables, and wireless media. In addition to communications with onsite field devices, the control center is commonly connected to external information sources

including the Internet and other control centers for gaining more support concerning accurate load forecasts and cooperative operations with external electric power systems in its critical decision-making processes. Firewalls are often deployed to separate internal communications from external networks. Firewalls are configured with stringent rules to only allow permissible data to flow into the microgrid cyber system while blocking potentially harmful data stemmed from unidentified external sources.

2.1 Cyber security Requirements

The microgrid cyber system collects, transmits, processes, displays, and stores the information on microgrid operations through data flows. Data appear in the form of monitoring and metering information, control commands, as well as microgrid configurations (e.g., network layout, communication protocol, device settings). Clearly, efficient and reliable data flows are essential for governing the continuous physical process.

In terms of the data pertaining to the cyber system, cyber security of microgrid operations ought to meet three fundamental requirements [2]: availability, integrity, and confidentiality, as stated below.

- Availability refers to guaranteeing that data are accessible and timely. It is vital to ensure a continued access to necessary data for making operational decisions so as to adapt swiftly to dynamic conditions in critical circumstances. Due to the time-sensitive nature of data, any latency or loss of synchronization may hamper the situational awareness and impact the operational performance of microgrids. Table1 lists the maximum latency allowed for multiple data types [3].

Table 1: Time latency requirement in microgrids [1]

Max Latency	Data Type
4ms	Protective relaying
Sub-seconds	PMU-based situational awareness monitoring
Seconds	Supervisory control and data acquisition
Minutes	Microgrid energy management
Hours	Smart meter reading

- Integrity refers to assuring that data are trustworthy and accurate. The authenticity and consistency of data should be retained over their entire life cycle, including collection by sensors, transmission via wired or wireless media, analysis in application servers, HMI visualization, and storage in the historian. Mean-while, data should always represent the actual information under all operating conditions. In particular, any data alterations by unauthorized parties need to be thwarted, which otherwise tend to incur adverse effects on microgrid functionalities.
- Confidentiality refers to protecting data from being accessed and comprehended by unauthorized parties. Any unexpected disclosure may reveal sensitive information with devastating outcomes on microgrid operations and customer behaviors.

The above cybersecurity requirements are differentiated from those in the traditional information technology (IT) domain. The IT security is encumbered with the burden of ensuring anonymity and confidentiality for preserving user privacy, whereas the primary focus of cybersecurity in microgrids is to retain the quality and the continuity of power supplies for keeping the lights on. Accordingly, availability and integrity are usually prioritized over confidentiality in order to maintain timely and reliable data flows for authorized applications that govern microgrid operations.

2.2 Cyber Vulnerabilities

Cyber vulnerabilities are flaws or weaknesses of a system that is exposed to cyber threats. Cyber vulnerabilities may exist across a microgrid cyber system, ranging from the application software, to the communication network, to field devices. Table 2 summarizes the most common cyber vulnerabilities. As cyber–physical systems, microgrids not only inherit common vulnerabilities from the IT domain, but also have to face unique vulnerabilities specific to their operational characteristics. In practice, communication technologies and networking components retain the same vulnerabilities as those used in the IT domain. However, field devices and software applications have their specific vulnerabilities which depend on the microgrid design and configuration.

Table 2 : Most Common Cyber Vulnerabilities in Microgrids [1]

Domain	Common Vulnerability
Application Software	Poor Code Quality
	Inadequate Configuration Management
	Poor Permissions and Access Management
	Inadequate Patch Management
	Inadequate Data Integrity Checking
	Inadequate Error Handling
	Inadequate Database Protection
Communication Network	Inadequate Segregation and Segmentation
	Inadequate Access Control
	Weak Intrusion Detection and Prevention
	Weak Encryption Mechanism
	Inadequate Sensitive Data Protection
	Inadequate Network Monitoring and Auditing
	Inadequate Anomaly Tracking
Field Devices	Unprotected Physical Access
	Improper Device Configuration
	Inadequate Firmware Protection
	Lack of Tamper-resistance Hardware
	Weak Authentication and Authorization

Microgrids tend to be susceptible to an increasing number of cyber vulnerabilities that result from the following trends.

- Growing complexity in communication technologies.
- Greater exposure to external networks.
- Increasingly extensive internal communications

2.3 Impact of Cyber Incidents on microgrid operations

Considering the complex cyber–physical interdependencies, cyber incidents cannot be viewed solely as IT activities. Any violation of availability, integrity, or confidentiality has the potential to impact the physical process. Sophisticated cyberattacks can even drive the operation of microgrids to collapse, resulting in substantial equipment damage and prolonged power outages.

Cyber incidents compromising availability or integrity tend to incur adverse effects on microgrid operations. These incidents may not only impact the efficiency and the economics of microgrid operations, but also threaten the continuity and the quality of power supplies. Although any violations of confidentiality might not pose direct physical consequences, they would help attackers prepare for subsequent attacks causing violations of availability or integrity. Figure 2 illustrates the impacts of cyberattacks on microgrid operations.

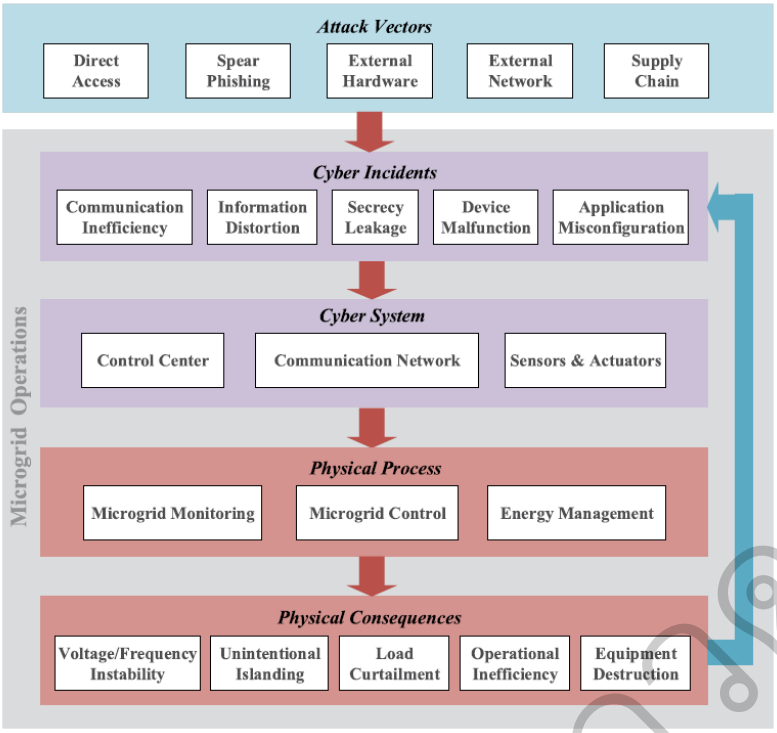

Figure 2 : The impacts of cyberattacks on microgrid operations [1].

2.4 Contractor responsibility

The Contractor's responsibilities shall include, but shall not be limited to:

1) The contractor shall provide designed and engineered of cybersecurity of microgrid operations to meet three fundamental requirements: availability, integrity, and confidentiality for MGBT for PEA approval.
2) The contractor shall supply all necessary materials and perform all necessary fabrication, testing, wiring, and interconnection work during the process of assembling and connecting to microgrid controller.
3) The contractor shall provide site acceptance testing (SAT) of every mode of operation of cyber security for microgrid system. SAT shall include the test sets in order to demonstrate the readiness of the cyber security system.
4) The contractor shall provide training PEA staff so that they will be self-sufficient in designing, testing, and maintaining the cyber security system.

References

[1] Z. Li, M. Shahidehpour, and F. Aminifar, "Cybersecurity in Distributed Power Systems," Proceeding of the IEEE , Vol. 105, No. 7, pp.1367-1388, July 2017.

[2] S. Sridhar, A. Hahn, and M. Govindarasu, "Cyber-physical system security for the electric power grid," Proceeding of the IEEE, Vol. 100, No. 1, pp. 210–224, Jan. 2012.

[3] NISTIR 7628: Guidelines for Microgrid Cyber Security: Microgrid Cyber Security Strategy, Architecture, and High-Level Requirements, The Microgrid Interoperability Panel– Cyber Security Working Group, 2010.

Appendix: Cyber Security Implementation Requirements

For the purposes of determining the applicability and scope of each of these requirements, the following terms and abbreviations are defined:

- BESS Battery Energy Storage System
- Gateway Communication Gateway
- GenSet Diesel Generator Set
- RCS Remote Control Switch
- MGC Microgrid controller
- MGIS Microgrid information system
- OP General Operations associate with the MGC

Each of the above includes all associated cyber assets together with all networking equipment, servers, workstations or other devices connected to their associated networks.

Cyber Asset An electronic device which uses a microprocessor. This includes servers, workstations, tablets, networking equipment, printers, IEDs, smart relays, smart meters, etc.

Capability The specified capability is to be included in cyber assets, software components, or supporting system, or the MGC design must provide the capability.

Configuration The cyber asset or system must be configured to provide this requirement.

Design The design of the system or system component must support this requirement. Depending on the design, this may affect components of the design.

Policy While all the following requirements reflect security policy, those items marked as "Policy" refer to additional requirements such as how configuration is to be determined or capabilities that may not be allowed.

Training Training to be developed including all class materials.

Procedure A procedure to support this requirement

Documentation Technical documentation to be created to support requirement

The following lists general comments for the security requirements.

(1) Contractor to assure that capability has been configured in accordance with the security policy prior to deployment on the production system.
(2) If a device or its managing system does not directly support this capability, compensating controls must be specified.

For the implementation of cyber security in the recommended MGC architecture, the awarded Contractor shall, with collaboration of PEA, implement necessary Cyber security capabilities. Contractor shall submit the security design to PEA for approval prior to implementation.

The microgrid information system shall have the capability to assign and enforce user privileges based on designated roles.

Type of control	Capability, Configuration
Where applied	MGC/BESS/GenSet/RCS/Gateway/OP
Applied to	All cyber assets and software that support user accounts.
Responsibility	Contractor
Comment	(1) (2)

The physical access control system, as described in related equipment as described in this TOR, shall provide audit records of successful, unsuccessful access attempts, which included the time, location and user identification information of the access event.

Type of control	Capability, Configuration
Where applied	MGC/BESS/GenSet/HighSpeedRCS/Gateway/OP
Applied to	All MGIS facilities.
Responsibility	Contractor
Comment	

1 Policies and Procedures

The section summarizes Cyber Security requirements that include policies, procedures, technology capabilities, system-wide or component-focused functionality. In each requirement, the applicable areas or systems are indicated for reference. At the end of this section, the table that summaries the expected responsible party of the requirements, e.g. either PEA or the Contractor(s), is included.

1.1 Microgrid Cyber Security Policies and Procedures

1.1.1 The Contractor shall, with PEA management support and guidance, and in accordance with NISTIR 7628 Guidelines for Smart Grid Cyber Security v1.0 – Aug 2010 or a later version, develop cyber security policies and procedures for the Microgrid information system.

Type of control	Policy development
Where applied	MGC/BESS/GenSet/RCS/Gateway/OP
Applies to	All operations, systems and cyber assets
Responsibility	Contractor to provide development guidance and support to PEA
Comment	

Type of control	Procedure development
Where applied	MGC/BESS/GenSet/RCS/Gateway/OP
Applies to	All operations, systems and cyber assets
Responsibility	Contractor to provide development guidance and support to PEA
Comment	

Policies are the overall specification of the security requirements of the system and its users. Procedures are a set of stated methods by which users will assure that the policy is being met. E.g. a policy may state that all personnel will have had background checks prior to be given access to the MGIS and there is a procedure for provisioning access that will at one point require that the background check be complete and meet PEAs documented requirement for the provisioning to proceed.

These policies must include, as appropriate, technical, procedural and administrative controls to achieve the policy goals.

These will apply to the organization and MGIS as a whole and will also include any policy items and procedures relevant to specific devices or subsystems.

Each of the items specified below must be included in the security policy and have associated procedures to manage them.

2 Access Control

2.1 Account Management

2.1.1 The Microgrid information system shall automatically terminate temporary and emergency accounts after an organization-defined time period for each type of account.

Type of control	Capability, Configuration
Where applied	MGC/BESS/GenSet/RCS/Gateway/OP
Applies to	All cyber assets and software that support user accounts.
Responsibility	Contractor
Comment	(1), (2)

2.1.2 The Microgrid information system shall automatically disable inactive accounts after an organization-defined time period. The awarded Contractor will discuss the use of single sign on at the start of the project in order to agree on the work process with PEA.

Type of control	Capability, Configuration
Where applied	MGC/BESS/GenSet/RCS/Gateway/OP
Applies to	All cyber assets that support user accounts.
Responsibility	Contractor, PEA
Comment	(1), (2)

2.1.3 The Microgrid information system shall automatically audit account creation, modification, disabling, and termination actions and notifies the required individuals. The awarded Contractor will discuss the use of single sign on at the start of the project in order to agree on the work process with PEA.

Type of control	Capability, Configuration
Where applied	MGC/BESS/GenSet/RCS/Gateway/OP
Applies to	All cyber assets that support user accounts.
Responsibility	Contractor
Comment	Devices or managing system must report this information for centralized monitoring. (1), (2)

2.2 Access Enforcement

2.2.1 The Microgrid information system enforces assigned authorizations for controlling access to the Microgrid information system in accordance with organization-defined policy and risk assessment**.**

Type of control	Capability
Where applied	MGC/BESS/GenSet/RCS/Gateway/OP
Applies to	All MGIS cyber assets meeting policy guidelines.
Responsibility	Contractor as required by PEA security policy
Comment	Best practices require that access to all cyber assets be restricted and controlled.

2.3 Least Privilege

2.3.1 The Microgrid information system shall enforce different levels of user privilege in interacting with the system.

Type of control	Capability, Configuration
Where applied	MGC/BESS/GenSet/RCS/Gateway/OP
Applies to	All cyber assets and software that support user accounts.
Responsibility	Contractor
Comment	(1) (2)

2.3.2 The Microgrid information system shall provide real-time logging and recording of the use of privileged accounts.

Type of control	Capability, Configuration
Where applied	MGC/BESS/GenSet/RCS/Gateway/OP
Applies to	All cyber assets and software that support user accounts.
Responsibility	Contractor
Comment	(1) (2)

2.4 Unsuccessful Login Attempts

2.4.1 The Microgrid information system shall enforce a login delay after a limited number of consecutive invalid login attempts.

Type of control	Capability, Configuration
Where applied	MGC/BESS/GenSet/RCS/Gateway/OP
Applies to	All cyber assets and software that support user accounts.
Responsibility	Contractor
Comment	(1)

2.4.2 The Microgrid information system shall provide real-time logging and recording of unsuccessful login attempts.

Type of control	Capability, Configuration
Where applied	MGC/BESS/GenSet/RCS/Gateway/OP
Applies to	All cyber assets and software that support user accounts.
Responsibility	Contractor
Comment	(1) (2)

2.4.3 The Microgrid information system shall provide real-time alerting to a management authority for the Microgrid information system when the number of defined consecutive invalid access attempts is exceeded.

Type of control	Capability
Where applied	MGC/BESS/GenSet/RCS/Gateway/OP
Applies to	All cyber assets and software that support user accounts.
Responsibility	Contractor
Comment	(1) (2)

2.5 Microgrid Information System Use Notification

2.5.1 The Microgrid information system shall display an approved system use notification message or banner before granting access to the Microgrid information system that provides privacy and security notices consistent with applicable laws, directives, policies, regulations, standards, and guidance.

Type of control	Capability, Configuration
Where applied	MGC/BESS/GenSet/RCS/Gateway/OP
Applies to	All cyber assets and software that support logon access at a human user interface.
Responsibility	Contractor
Comment	(1) (2)

2.6 Previous Logon Notification

2.6.1 The Microgrid information system shall, notify the user, upon successful logon, of the date and time of the last logon and the number of unsuccessful logon attempts since the last successful logon.

Type of control	Capability, Configuration
Where applied	MGC/BESS/GenSet/RCS/Gateway/OP
Applies to	MGIS workstations and servers, and where feasible, any cyber assets or software that support logon access at a human user interface.
Responsibility	Contractor
Comment	(1) (2)

2.7 Concurrent Session Control

2.7.1 The Microgrid information system shall limit the number of concurrent sessions for any user on the Microgrid information system

Type of control	Capability, Configuration
Where applied	MGC/BESS/GenSet/RCS/Gateway/OP
Applies to	MGIS workstations and servers.
Responsibility	Contractor
Comment	(1) (2)

2.8 Session Lock

2.8.1 The Microgrid information system shall, where feasible, after a defined period of inactivity or when the logged on user is away from the system, lock user access to the system.

Type of control	Capability, Configuration
Where applied	MGC/BESS/GenSet/RCS/Gateway/OP
Applies to	All cyber assets and software that support interactive user interfaces.
Responsibility	Contractor
Comment	(1) (2)

2.8.2 The Microgrid information system shall retain the session lock until an authorized user reestablishes access using appropriate identification and authentication procedures.

Type of control	Capability, Configuration
Where applied	MGC/BESS/GenSet/RCS/Gateway/OP
Applies to	All cyber assets and software that support interactive user interfaces.
Responsibility	Contractor
Comment	(1) (2)

2.9 Remote Session Termination

2.9.1 The Microgrid information system shall terminate a remote session at the end of the session or after a period of inactivity.

Type of control	Capability, Configuration
Where applied	MGC/BESS/GenSet/RCS/Gateway/OP
Applies to	All cyber assets and software that support interactive user interfaces.
Responsibility	Contractor
Comment	(1) (2)

2.10 Remote Access

2.10.1 The Microgrid information system shall authorize, monitor, and manage all methods of remote access to the Microgrid information system.

Type of control	Capability, Configuration
Where applied	MGC/BESS/GenSet/RCS/Gateway/OP
Applies to	All cyber assets and software that support remote access into the MGIS.
Responsibility	Contractor
Comment	(1) (2)

2.10.2 The Microgrid information system shall authenticate remote access, and to protect the confidentiality and integrity of remote access sessions.

Type of control	Capability, Configuration
Where applied	MGC/BESS/GenSet/RCS/Gateway/OP
Applies to	All cyber assets and software that support remote access into the MGIS.
Responsibility	Contractor
Comment	(1) (2)

2.10.3 The Microgrid information system shall route all remote accesses through a limited number of managed access control points.

Type of control	Capability, Configuration
Where applied	MGC/BESS/GenSet/RCS/Gateway/OP
Applies to	All cyber assets and software that support remote access into the MGIS.
Responsibility	Contractor
Comment	(1) (2) Contractor design must route all remote access through managed access points (e.g. firewalls), and said design must provide, implement and configure.

2.10.4 The Microgrid information system shall protect wireless access to the Microgrid information system using authentication and encryption. Note: Authentication applies to user, device, or both as necessary.

Type of control	Capability, Configuration
Where applied	MGC/BESS/GenSet/RCS/Gateway/OP
Applies to	All wireless communications to the MGIS.
Responsibility	Contractor
Comment	(1) (2), authentication applies to both users and devices.

2.10.5 The Microgrid information system shall monitor for unauthorized remote connections to the Microgrid information system.

Type of control	Capability, Configuration
Where applied	MGC/BESS/GenSet/RCS/Gateway/OP
Applies to	All cyber assets and software that support remote access into the MGIS.
Responsibility	Contractor
Comment	(1) (2), Contractor design must include capability to report unauthorized connections to appropriate PEA personnel. Monitoring to be done at access points into the MGIS. Direct wireless access to MGIS cyber assets requires monitoring at the accessed device.

2.10.6 The Contractor shall enable remote access to Microgrid information system component locations (e.g., control center, field locations) only when necessary, approved, authenticated, and for the duration necessary.

Type of control	Policy
Where applied	MGC/BESS/GenSet/RCS/Gateway/OP
Applies to	All wireless communications to the MGIS.
Responsibility	Contractor
Comment	

2.10.7 The Microgrid information system shall employ automated mechanisms to facilitate the monitoring and control of remote access methods.

Type of control	Capability
Where applied	MGC/BESS/GenSet/RCS/Gateway/OP
Applies to	All wireless communications to the MGIS.
Responsibility	Contractor
Comment	(1) (2) Contractor design must include capability to monitor and control remote access.

2.10.8 The Contractor shall disable, when not intended for use, wireless networking capabilities internally embedded within Microgrid information system components.

Type of control	Capability, Configuration
Where applied	MGC/BESS/GenSet/RCS/Gateway/OP
Applies to	All cyber assets in the MGIS with wireless networking capabilities.
Responsibility	Contractor
Comment	(1) (2)

2.11 Wireless Access Restrictions

2.11.1 Where wireless networks are used, the Microgrid information system shall use separate wireless networks for control system, business and guest access.

Type of control	Capability, Configuration
Where applied	MGC/BESS/GenSet/RCS/Gateway/OP
Applies to	All cyber assets in the MGIS with wireless networking capabilities.
Responsibility	Contractor
Comment	(1) (2), Contractor design and implementation must include capability to segregate wireless network traffic.

2.11.2 Where wireless networks are used for other than control system communications, the Microgrid information system shall use WPA2-Enterprise or stronger.

Type of control	Capability, Configuration
Where applied	MGC/BESS/GenSet/RCS/Gateway/OP
Applies to	All non-control system cyber assets associated with the MGIS with wireless networking capabilities.
Responsibility	Contractor
Comment	(1) (2)

2.12 Access Control for Portable and Mobile Devices

2.12.1 The Contractor shall disable on all Microgrid information system devices physical ports that can accept removable media when not intended for use.

Type of control	Configuration
Where applied	MGC/BESS/GenSet/RCS/Gateway/OP
Applies to	All cyber assets associated with the MGIS.
Responsibility	Contractor
Comment	(1) (2)

2.13 Control System Access Restrictions

2.13.1 The Microgrid information system shall employ mechanisms in the MGIS design and implementation to restrict access from PEA's enterprise network. Connections should be proxied through an intervening DMZ.

Type of control	Design, Capability, Configuration
Where applied	MGC/BESS/GenSet/RCS/Gateway/OP
Applies to	All cyber assets associated with the MGIS.
Responsibility	Contractor
Comment	(1) (2)

2.13.2 The Microgrid information system shall implement mechanisms to restrict access to the Microgrid information system from PEA's enterprise network to read-only.

Type of control	Configuration
Where applied	MGC/BESS/GenSet/RCS/Gateway/OP
Applies to	All cyber assets associated with the MGIS.
Responsibility	Contractor
Comment	(1) (2)

2.14 Publicly Accessible Content

2.14.1 The Contractor shall remove all nonpublic information from the publicly accessible information systems in the Microgrid information system.

Type of control	Configuration
Where applied	MGC/BESS/GenSet/RCS/Gateway/OP
Applies to	All cyber assets associated with the MGIS.
Responsibility	Contractor
Comment	(1) (2)

2.15 Passwords

2.15.1 The Microgrid information system shall, where feasible, employ username and password combinations to gain access to Microgrid information system assets.

Type of control	Capability, Configuration
Where applied	MGC/BESS/GenSet/RCS/Gateway/OP
Applies to	All MGIS cyber assets which provide user access.
Responsibility	Contractor
Comment	(1) (2), devices that allow unauthenticated access should not be used, but may be allowed if no feasible alternative exists and the documented risk is understood and compensating controls are deployed.

2.15.2 Passwords shall be a minimum of 8 characters long and contain a combination of uppercase, lowercase, numeric, and special characters, or using an alternative means be of greater strength.

Type of control	Capability, Configuration
Where applied	MGC/BESS/GenSet/RCS/Gateway/OP
Applies to	All cyber assets and software that use passwords for authentication.
Responsibility	Contractor
Comment	(1) (2), where feasible stronger password configuration should be considered.

2.15.3 The Microgrid information system shall not allow direct user logins using privileged (e.g. with administrator or root) accounts.

Type of control	Configuration
Where applied	MGC/BESS/GenSet/RCS/Gateway/OP
Applies to	All cyber assets and software that support user accounts.
Responsibility	Contractor
Comment	(1) (2), by requirement 2.3.1 privilege levels are assumed to be enabled.

2.15.4 Passwords shall expire automatically after an organization defined period of time.

Type of control	Configuration, Procedure
Where applied	MGC/BESS/GenSet/RCS/Gateway/OP
Applies to	Workstations, servers, centrally manage access control systems, and where feasible, any MGIS cyber assets or software that support user accounts.
Responsibility	Contractor as required by PEA security policy
Comment	(1) (2), where no technical control is feasible, procedural controls must be used.

3 Awareness and Training

3.1 Security Awareness Training

3.1.1 The Contractor shall, with PEA management support and guidance, develop a cyber security awareness and training program for the Microgrid information system.

Type of control	Training, Documentation
Where applied	MGC/BESS/GenSet/RCS/Gateway/OP
Applies to	Overall MGIS, Training specifics will vary by system
Responsibility	Contractor with PEA support
Comment	

4 Audit and Accountability

4.1 Auditable Events

4.1.1 The Contractor shall, with PEA management support and guidance, develop a lists of auditable events for the Microgrid information system

Type of control	Documentation
Where applied	MGC/BESS/GenSet/RCS/Gateway/OP
Applies to	All MGIS cyber assets
Responsibility	Contractor
Comment	

4.1.2 The list of auditable events shall be based on risk assessment

Type of control	Policy
Where applied	MGC/BESS/GenSet/RCS/Gateway/OP
Applies to	All MGIS cyber assets
Responsibility	Contractor and PEA
Comment	This requirement expands 4.1.1

4.1.3 The list of auditable events shall include execution of privileged functions

Type of control	Policy
Where applied	MGC/BESS/GenSet/RCS/Gateway/OP
Applies to	All MGIS cyber assets
Responsibility	Contractor
Comment	This requirement expands 4.1.1

4.2 Content of Audit Records

4.2.1 The Microgrid information system shall generate audit records that at a minimum provide for each event, the date and time of the event, device or component where the event occurred, the type of event, user/subject identity, and the outcome of the event.

Type of control	Capability, Configuration
Where applied	MGC/BESS/GenSet/RCS/Gateway/OP
Applies to	All MGIS cyber assets.
Responsibility	Contractor
Comment	(1) (2)

4.3 Time Stamps

4.3.1 The Microgrid information system shall use internal system clocks to generate time stamps for audit records and that the system synchronizes internal Microgrid information system clocks on an organization-defined frequency using an organization-defined time source.

Type of control	Capability, Configuration
Where applied	MGC/BESS/GenSet/RCS/Gateway/OP
Applies to	All MGIS cyber assets
Responsibility	Contractor, PEA
Comment	(1), (2)

5 Security Assessment and Authorization

5.1 Microgrid Information System Connections

5.1.1 The Contractor shall identify, document and protect from tampering or damage, all external Microgrid information system and communication connections.

Type of control	Capability, Configuration
Where applied	MGC/BESS/GenSet/RCS/Gateway/OP
Applies to	All MGIS cyber assets
Responsibility	Contractor
Comment	

6 Configuration Management

6.1 Component Inventory

6.1.1 The Contractor shall provide an accurate inventory of all Microgrid information system components (devices and software) and their base-line configuration settings, either individually or by component class.

Type of control	Documentation
Where applied	MGC/BESS/GenSet/RCS/Gateway/OP
Applies to	All MGIS cyber assets and installed software
Responsibility	Contractor
Comment	

6.2 Factory Default Settings Management

6.2.1 The Contractor shall replace default usernames and passwords whenever possible.

Type of control	Configuration
Where applied	MGC/BESS/GenSet/RCS/Gateway/OP
Applies to	All MGIS cyber assets
Responsibility	Contractor
Comment	(1), (2); when not possible, the details must be documented and approved by PEA.

7 Identification and Authorization

7.1 Authenticator Management

7.1.1 Define initial authentication credential content, such as defining password length and composition, tokens; and establish administrative procedures for initial authentication credential distribution; lost, compromised, or damaged authentication credentials; and revoking authentication.

Type of control	Configuration, Procedure
Where applied	MGC/BESS/GenSet/RCS/Gateway/OP
Applies to	All MGIS cyber assets
Responsibility	Contractor, PEA
Comment	(1)

7.1.2 Authentication credentials on publicly accessible devices (e.g smart meters) shall use shall be unique to each device. On other assets, the use of non-unique credentials shall be minimized where feasible.

Type of control	Capability, Configuration
Where applied	MGC/BESS/GenSet/RCS/Gateway/OP
Applies to	All MGIS cyber assets
Responsibility	Contractor, PEA
Comment	(1), (2)

7.2 User Identification and Authorization

7.2.1 The Microgrid information system shall use multifactor authentication for (1) Remote access to non-privileged accounts, (2) local access to privileged accounts, and (3) remote access to privileged accounts.

Type of control	Capability, Configuration
Where applied	MGC/BESS/GenSet/RCS/Gateway/OP
Applies to	All MGIS cyber assets and software supporting authenticated user access
Responsibility	Contractor
Comment	(1), (2)

7.3 Device Identification and Authentication

7.3.1 The Microgrid information system shall uniquely identify and authenticate devices against an organization-defined list of approved devices before establishing a connection.

Type of control	Capability, Configuration
Where applied	MGC/BESS/GenSet/RCS/Gateway/OP
Applies to	All MGIS cyber assets
Responsibility	Contractor, PEA
Comment	(1), (2)

7.3.2 The Microgrid information system shall authenticate devices before establishing remote network connections using bidirectional authentication between devices.

Type of control	Capability, Configuration
Where applied	MGC/BESS/GenSet/RCS/Gateway/OP
Applies to	All MGIS cyber assets
Responsibility	Contractor
Comment	(1), (2)

7.4 Authenticator Feedback

7.4.1 Authentication mechanisms in the Microgrid information system shall obscure feedback of authentication information during the authentication process.

Type of control	Capability, Configuration
Where applied	MGC/BESS/GenSet/RCS/Gateway/OP
Applies to	All MGIS cyber assets with interactive authentication
Responsibility	Contractor
Comment	(1), (2)

8 Information and Document Management

8.1 Information Exchange

8.1.1 When a specific device is required to communicate with another device outside the Microgrid information system, communications shall be limited to only the devices that need to communicate.

Type of control	Configuration
Where applied	MGC/BESS/GenSet/RCS/Gateway/OP
Applies to	All MGIS cyber assets
Responsibility	Contractor
Comment	(1), (2)

9 Incident Response

9.1 Incident Handling

9.1.1 The Microgrid information system shall employ automated mechanisms to assist in the tracking of security incidents and in the collection and analysis of incident information.

Type of control	Capability, Configuration
Where applied	MGC/BESS/GenSet/RCS/Gateway/OP
Applies to	All MGIS cyber assets
Responsibility	Contractor
Comment	

9.2 Microgrid Information System Backup

9.2.1 The Microgrid information system shall create backups. If the design to support this requirement needs hardware or software to be deployed, this is the Contractor's responsibility.

Type of control	Capability, Configuration
Where applied	MGC/BESS/GenSet/RCS/Gateway/OP
Applies to	All MGIS cyber assets
Responsibility	Contractor
Comment	This includes user-level information, system-level information, and documentation as needed to recover the system, and that the integrity and confidentiality of the backup information be protected.

10 System Development and Maintenance

10.1 Maintenance Personnel

10.1.1 Remote maintenance sessions into the Microgrid information system shall be protected through the use of a strong authentication credentials.

Type of control	Capability, Configuration
Where applied	MGC/BESS/GenSet/RCS/Gateway/OP
Applies to	All MGIS cyber assets and systems allowing remote maintenance
Responsibility	Contractor
Comment	(1), (2)

11 Physical and Environmental Security

11.1 Physical Access Control Authorizations

11.1.1 The Contractor shall implement physical access control mechanisms requiring multifactor authentication to gain access to the facility where the Microgrid information system resides. The system shall be installed at the existing facility.

Type of control	Capability, Configuration
Where applied	MGC/BESS/GenSet/RCS/Gateway/OP
Applies to	MGIS control rooms, or facilities housing MGIS servers, workstations, routers, security appliances (e.g. IDS, firewalls), or assets used in access control or monitoring of the MGIS.
Responsibility	PEA
Comment	

11.2 Physical Access Control

11.2.1 The Contractor shall employ hardware to deter unauthorized physical access control to Microgrid information system devices. The system shall be installed at the existing facility.

Type of control	Capability, Configuration
Where applied	MGC/BESS/GenSet/RCS/Gateway/OP
Applies to	All MGIS cyber assets
Responsibility	PEA
Comment	All assets should be physically protected, or tamper resistant with tamper detection.

11.2.2 The Contractor shall employ measures to ensure that every physical access control point to the facility where the Microgrid information system resides is guarded or alarmed and monitored on an organization-defined frequency.

Type of control	Capability, Configuration
Where applied	MGC/BESS/GenSet/RCS/Gateway/OP
Applies to	All physical access control points of MGIS facilities.
Responsibility	Contractor, PEA
Comment	

11.3 Monitoring Physical Access Control

11.3.1 The Contractor shall install real-time physical intrusion alarms and surveillance equipment to protect access to facilities where the Microgrid information systems reside. The system shall be installed at the existing facility.

Type of control	Capability, Configuration
Where applied	MGC/BESS/GenSet/RCS/Gateway/OP
Applies to	All MGIS facilities.
Responsibility	PEA
Comment	

11.4 Emergency Power

11.4.1 The Contractor shall implement an alternate power supply to facilitate an orderly shutdown of noncritical Microgrid information system components in the event of a primary power source loss.

Type of control	Capability, Configuration
Where applied	MGC/BESS/GenSet/RCS/Gateway/OP
Applies to	All noncritical MGIS components, excluding those for which loss of power would not adversely affect the MGIS or the MGIS component.
Responsibility	Contractor
Comment	

11.4.2 For self-contained Microgrid information system components not reliant on external power generation, the Contractor shall implement alternate power supply for long-term operation. The awarded Contractor will agree on the details with PEA later before the start of the project as PEA will provide the power sources.

Type of control	Capability, Configuration
Where applied	MGC/BESS/GenSet/RCS/Gateway/OP
Applies to	All MGIS components not reliant on external power generation.
Responsibility	Contractor
Comment	

11.5 Location of Microgrid Information System Assets

11.5.1 Microgrid information system assets shall be located to minimize potential damage from physical and environmental hazards.

Type of control	Design
Where applied	MGC/BESS/GenSet/RCS/Gateway/OP
Applies to	Overall design of MGIS
Responsibility	Contractor
Comment	

12 Risk Management and Assessment

12.1 Risk Assessment

12.1.1 The Contractor shall provide the results of a cyber security risk assessment from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and Microgrid information systems of the proposed system design.

Type of control	Documentation
Where applied	MGC/BESS/GenSet/RCS/Gateway/OP
Applies to	Overall design of MGIS
Responsibility	Contractor
Comment	

12.1.2 The Contractor shall use the risk assessment to determine the types of security protection and their configuration for the Microgrid information system.

Type of control	Design
Where applied	MGC/BESS/GenSet/RCS/Gateway/OP
Applies to	Overall design of MGIS
Responsibility	Contractor
Comment	

13 Services Acquisition

13.1 Software License Usage Restrictions

13.1.1 The Contractor shall use software and associated documentation in accordance with contract agreements and applicable copyright laws.

Type of control	Policy
Where applied	MGC/BESS/GenSet/RCS/Gateway/OP
Applies to	All MGIS cyber assets
Responsibility	Contractor
Comment	Contractor to provide documentation of how this requirement is met.

13.2 Security Engineering Principles

13.2.1 The Contractor shall require the Microgrid information system and its components to be created or modified using secure engineering practices.

Type of control	Policy
Where applied	MGC/BESS/GenSet/RCS/Gateway/OP
Applies to	All MGIS cyber assets
Responsibility	Contractor, PEA
Comment	Contractor to provide documentation of how this requirement is met.

14 Communication Protection

14.1 Communications Partitioning

14.1.1 The Microgrid information system shall partition the communications for telemetry/data acquisition services and management functionality.

Type of control	Design
Where applied	MGC/BESS/GenSet/RCS/Gateway/OP
Applies to	All MGIS cyber assets
Responsibility	Contractor
Comment	(2)

14.2 Security Function Isolation

14.2.1 The Microgrid information system shall isolate security functions from non-security functions.

Type of control	Capability, Design
Where applied	MGC/BESS/GenSet/RCS/Gateway/OP
Applies to	All MGIS cyber assets
Responsibility	Contractor
Comment	(2)

14.3 Denial-of-Service Protection

14.3.1 The Microgrid information system shall mitigate or limit the effects of denial-of-service attacks based on an organization-defined list of denial-of-service attacks.

Type of control	Design, Configuration
Where applied	MGC/BESS/GenSet/RCS/Gateway/OP
Applies to	All MGIS cyber assets
Responsibility	Contractor, PEA
Comment	Involves at minimum configuring network perimeter devices to filter traffic. List of denial-of-service attacks to be determined based on risk assessment.

14.3.2 The Microgrid information system shall restrict the ability of users to launch denial-of-service attacks against other Microgrid information systems or networks.

Type of control	Design, Configuration
Where applied	MGC/BESS/GenSet/RCS/Gateway/OP
Applies to	All MGIS cyber assets
Responsibility	Contractor
Comment	Involves at minimum configuring network devices to outbound traffic at the MGIS perimeter and traffic between key internal boundaries.

14.4 Boundary Protection

14.4.1 The Microgrid information system shall have a defined and documented boundary of the Microgrid information system. The awarded Contractor will agree on the details with PEA later before the start of the project as PEA will provide the existing information.

Type of control	Design, Documentation
Where applied	MGC/BESS/GenSet/RCS/Gateway/OP
Applies to	All MGIS cyber assets
Responsibility	Contractor
Comment	

14.4.2 The Microgrid information system shall monitor and control communications at the external boundary of the system and at key internal boundaries within the system.

Type of control	Design
Where applied	MGC/BESS/GenSet/RCS/Gateway/OP
Applies to	All MGIS cyber assets
Responsibility	PEA and Contractor
Comment	

14.4.3 The Microgrid information system connects to external networks or information systems only through managed interfaces consisting of boundary protection devices.

Type of control	Design, Configuration, Capability
Where applied	MGC/BESS/GenSet/RCS/Gateway/OP
Applies to	All MGIS cyber assets
Responsibility	Contractor
Comment	Requires all boundary assets to be managed devices (e.g. proxies, gateways, firewalls)

14.4.4 The managed interface implements security measures appropriate for the protection of integrity and confidentiality of the transmitted information

Type of control	Policy, Configuration
Where applied	MGC/BESS/GenSet/RCS/Gateway/OP
Applies to	All MGIS cyber assets
Responsibility	Contractor
Comment	

14.4.5 The Contractor shall configure the Microgrid information system to prevent public or other external access into the organization's internal Microgrid information system networks except as appropriately mediated.

Type of control	Configuration
Where applied	MGC/BESS/GenSet/RCS/Gateway/OP
Applies to	All MGIS cyber assets
Responsibility	Contractor
Comment	

14.4.6 The Microgrid information system shall be configured to deny network traffic by default and allow network traffic by exception (i.e., deny all, permit by exception).

Type of control	Configuration
Where applied	MGC/BESS/GenSet/RCS/Gateway/OP
Applies to	All MGIS cyber assets
Responsibility	Contractor
Comment	(1), (2)

14.4.7 The Microgrid information system shall check incoming communications to ensure that the communications are coming from an authorized source and routed to an authorized destination.

Type of control	Configuration
Where applied	MGC/BESS/GenSet/RCS/Gateway/OP
Applies to	All MGIS cyber assets
Responsibility	Contractor
Comment	(1), (2)

14.5 Communication Integrity

14.5.1 The Microgrid information system shall protect the integrity of electronically communicated information including during aggregation, packaging, and transformation in preparation for transmission.

Type of control	Policy
Where applied	MGC/BESS/GenSet/RCS/Gateway/OP
Applies to	All MGIS cyber assets
Responsibility	Contractor
Comment	(1), (2)

14.5.2 The Microgrid information system shall employ cryptographic mechanisms to ensure integrity.

Type of control	Policy
Where applied	MGC/BESS/GenSet/RCS/Gateway/OP
Applies to	All MGIS cyber assets
Responsibility	Contractor
Comment	

14.6 Communication Confidentiality

14.6.1 The Microgrid information system protects the confidentiality of communicated information.

Type of control	Policy
Where applied	MGC/BESS/GenSet/RCS/Gateway/OP
Applies to	All MGIS cyber assets
Responsibility	Contractor
Comment	

14.6.2 The Microgrid information system shall employ cryptographic mechanisms to prevent unauthorized disclosure of information during transmission.

Type of control	Policy
Where applied	MGC/BESS/GenSet/RCS/Gateway/OP
Applies to	All MGIS cyber assets
Responsibility	Contractor
Comment	

14.7 Use of Validated Cryptography

14.7.1 All of the cryptography and other security functions (e.g., hashes, random number generators, etc.) that are required for use in the Microgrid information system shall be limited to those algorithms that have received substantial public review and have been proven to work effectively.

Type of control	Policy
Where applied	MGC/BESS/GenSet/RCS/Gateway/OP
Applies to	All MGIS cyber assets
Responsibility	Contractor
Comment	

14.8 Public Key Infrastructure Certificates

14.8.1 For Microgrid information systems that implement a public key infrastructure, the organization issues public key certificates under an appropriate certificate policy or obtains public key certificates under an appropriate certificate policy from a PEA approved service provider.

Type of control	Policy
Where applied	MGC/BESS/GenSet/RCS/Gateway/OP
Applies to	All MGIS cyber assets
Responsibility	Contractor
Comment	

14.9 Mobile Code

14.9.1 The Microgrid information system shall have the capability to document, monitor, and manage the use of mobile code within the Microgrid information system.

Type of control	Design
Where applied	MGC/BESS/GenSet/RCS/Gateway/OP
Applies to	All MGIS cyber assets
Responsibility	Contractor
Comment	Mobile code technologies include, for example, Java, JavaScript, ActiveX, PDF, Postscript, Shockwave movies, Flash animations, and VBScript

14.9.2 The Microgrid information system shall implement detection and inspection mechanisms to identify unauthorized mobile code and takes corrective actions, when necessary.

Type of control	Design, Capability
Where applied	MGC/BESS/GenSet/RCS/Gateway/OP
Applies to	All MGIS workstations, mobile devices, or any cyber asset using mobile code.
Responsibility	Contractor
Comment	

14.10 System Connections

14.10.1 All external Microgrid information system and communication connections are identified and protected from tampering or damage.

Type of control	Design, Capability
Where applied	MGC/BESS/GenSet/RCS/Gateway/OP
Applies to	All MGIS communication connections
Responsibility	Contractor
Comment	(2);

14.10.2 External access point connections to the Microgrid information system shall be secured. Access points include any externally connected communication end point (for example, dial-up modems).

Type of control	Design, Capability
Where applied	MGC/BESS/GenSet/RCS/Gateway/OP
Applies to	All MGIS communication connections
Responsibility	Contractor
Comment	(2);

14.11 Security Roles

14.11.1 The Microgrid information system design and implementation shall specify the security roles and responsibilities for the users of the Microgrid information system.

Type of control	Design, Configuration
Where applied	MGC/BESS/GenSet/RCS/Gateway/OP
Applies to	All MGIS systems
Responsibility	PEA
Comment	Roles and responsibilities to be based on information sensitivity. Roles to be defined based on job descriptions or for individuals.

14.12 Message Authenticity

14.12.1 The Microgrid information system shall provide mechanisms to protect the authenticity of device-to-device communications, including message authentication mechanisms at the protocol level for both serial and routable protocols.

Type of control	Design, Capability
Where applied	MGC/BESS/GenSet/RCS/Gateway/OP
Applies to	All MGIS device communications
Responsibility	Contractor
Comment	Message authentication provides protection from malformed traffic, misconfigured devices, and malicious entities.

14.13 Secure Name/Address Resolution Service

14.13.1 Systems that provide name/address resolution shall be configured to supply additional data origin and integrity artefacts along with the authoritative data returned in response to resolution queries.

Type of control	Configuration
Where applied	MGC/BESS/GenSet/RCS/Gateway/OP
Applies to	All MGIS name/address resolution services
Responsibility	Contractor
Comment	Name resolution services (e.g. DNS) to be configured to provide additional security information to requesting device.

14.13.2 Systems that provide name/address resolution when operating as part of a distributed, hierarchical namespace, shall provide the means to indicate the security status of child subspaces and, if the child supports secure resolution services, enabled verification of a chain of trust among parent and child domains.

Type of control	Configuration
Where applied	MGC/BESS/GenSet/RCS/Gateway/OP
Applies to	All MGIS name/address resolution services
Responsibility	Contractor
Comment	Name resolution services (e.g. DNS) to be configured to provide additional security information to requesting device.

14.14 Fail in Known State

14.14.1 The Microgrid information system shall fail to a known state for defined failures.

Type of control	Design, Configuration
Where applied	MGC/BESS/GenSet/RCS/Gateway/OP
Applies to	All MGIS cyber assets
Responsibility	Contractor
Comment	Addresses safety and security. Required of system design and configuration to prevent injury, damage, or compromise of security.

14.15 Microgrid Information System Partitioning

14.15.1 The Microgrid information system shall be partitioned into components residing in separate physical or logical domains (or environments).

Type of control	Design, Configuration
Where applied	MGC/BESS/GenSet/RCS/Gateway/OP
Applies to	All MGIS cyber assets
Responsibility	Contractor
Comment	MGIS components of varying security classes to be in separate domains. Components from different MGIS systems to be in separate domains.

15 Information Integrity

15.1 Malicious Code and Spam Protection

15.1.1 The Microgrid information system shall implement malicious code protection mechanisms.

Type of control	Design, Configuration
Where applied	MGC/BESS/GenSet/RCS/Gateway/OP
Applies to	All MGIS cyber assets
Responsibility	Contractor
Comment	May be implemented at device or system level as appropriate. (2)

15.1.2 The Microgrid information system shall update malicious code protection mechanisms (including signature definitions) whenever new releases are available in accordance with organizational configuration management policy and procedures.

Type of control	Design, Configuration
Where applied	MGC/BESS/GenSet/RCS/Gateway/OP
Applies to	All MGIS cyber assets
Responsibility	Contractor to update all malicious code protection mechanisms to available releases prior to deployment, PEA to manage thereafter.
Comment	

15.1.3 The Microgrid information system shall prevent users from circumventing malicious code protection capabilities.

Type of control	Design, Configuration
Where applied	MGC/BESS/GenSet/RCS/Gateway/OP
Applies to	All MGIS cyber assets
Responsibility	Contractor
Comment	

15.1.4 Malicious code protection mechanisms in the Microgrid information system shall be centrally managed.

Type of control	Design, Capability, Configuration
Where applied	MGC/BESS/GenSet/RCS/Gateway/OP
Applies to	All MGIS malicious code protection mechanisms
Responsibility	Contractor
Comment	

15.1.5 The use of mechanisms to centrally manage malicious code protection must not degrade the operational performance of the Microgrid information system

Type of control	Design, Configuration
Where applied	MGC/BESS/GenSet/RCS/Gateway/OP
Applies to	All MGIS malicious code protection mechanisms
Responsibility	Contractor
Comment	

15.1.6 The Microgrid information system shall employ spam protection mechanisms at system entry points and at workstations, servers, or mobile computing devices on the network to detect and take action on unsolicited messages transported by electronic mail, electronic mail attachments, Web accesses, or other common means.

Type of control	Design, Configuration
Where applied	MGC/BESS/GenSet/RCS/Gateway/OP
Applies to	All MGIS entry points, workstations, servers, mobile computing devices on MGIS network
Responsibility	Contractor
Comment	

15.2 Microgrid Information System Monitoring Tools and Techniques

15.2.1 The Contractor shall employ mechanisms to allow events on the Microgrid information system to be monitored to detect attacks, unauthorized activities or conditions, and non-malicious errors.

Type of control	Design, Capability
Where applied	MGC/BESS/GenSet/RCS/Gateway/OP
Applies to	All devices on MGIS network; information obtained from intrusion monitoring tools
Responsibility	Contractor
Comment	Includes implementation of a security event monitoring system and intrusion detection system.

15.2.2 In response to detected activity, the Microgrid information system shall notify a defined list of incident response personnel

Type of control	Design, Configuration
Where applied	MGC/BESS/GenSet/RCS/Gateway/OP
Applies to	MGIS intrusion monitoring tools
Responsibility	Contractor
Comment	

15.2.3 The Contractor shall configure the Microgrid information system to protect information obtained from intrusion monitoring tools from unauthorized access, modification, and deletion.

Type of control	Configuration
Where applied	MGC/BESS/GenSet/RCS/Gateway/OP
Applies to	information obtained from intrusion monitoring tools
Responsibility	Contractor
Comment	

15.2.4 Individual intrusion detection tools shall be interconnected and configured into a Microgrid system-wide intrusion detection system using common protocols.

Type of control	Design, Configuration
Where applied	MGC/BESS/GenSet/RCS/Gateway/OP
Applies to	MGIS intrusion detection system
Responsibility	Contractor
Comment	

15.2.5 The Microgrid information system shall provide a real-time alert when indications of compromise or potential compromise occur.

Type of control	Design, Capability
Where applied	MGC/BESS/GenSet/RCS/Gateway/OP
Applies to	MGIS security information and event management system / intrusion detection system
Responsibility	Contractor
Comment	

15.2.6 The Microgrid information system prevents users from circumventing host-based intrusion detection and prevention capabilities.

Type of control	Design, Configuration
Where applied	MGC/BESS/GenSet/RCS/Gateway/OP
Applies to	MGIS host based IDS/IPS
Responsibility	Contractor
Comment	

15.2.7 The Microgrid information system shall provide logging usage data for at least 90 days according to Thai ICT law.

Type of control	Design, Capability
Where applied	MGC/BESS/GenSet/RCS/Gateway/OP
Applies to	All devices on MGIS network.
Responsibility	Contractor
Comment	

15.3 Security Alerts and Advisories

15.3.1 The Microgrid information system shall receive Microgrid information system security alerts, advisories, and directives from external organizations.

Type of control	Design, Procedure
Where applied	MGC/BESS/GenSet/RCS/Gateway/OP
Applies to	MGIS operations
Responsibility	Contractor to assist PEA in determining appropriate information sources and procedure to receive
Comment	Security information on all MGIS components and systems must be monitored.

15.3.2 The Microgrid information system shall generate and disseminate internal security alerts, advisories, and directives as deemed necessary.

Type of control	Capability, Configuration
Where applied	MGC/BESS/GenSet/RCS/Gateway/OP
Applies to	MGIS security information and event management system / intrusion detection system, and security information obtained by personnel from other sources
Responsibility	Contractor
Comment	

15.3.3 The Microgrid information system shall employ automated mechanisms to disseminate security alert and advisory information throughout the organization.

Type of control	Capability, Configuration
Where applied	MGC/BESS/GenSet/RCS/Gateway/OP
Applies to	MGIS security information and event management system / intrusion detection system, and security information obtained by personnel from other sources
Responsibility	Contractor
Comment	

15.4 Security Functionality Verification

15.4.1 The Microgrid information system provide the capability to allow the organization, upon Microgrid information system startup and restart, to verify the correct operation of security functions within the Microgrid information system.

Type of control	Capability
Where applied	MGC/BESS/GenSet/RCS/Gateway/OP
Applies to	All MGIS security functions
Responsibility	Contractor
Comment	(2)

15.5 Information Input Validation

15.5.1 The Microgrid information system shall employ mechanisms to check the accuracy, completeness, validity, and authenticity of information input to the system.

Type of control	Capability, Configuration
Where applied	MGC/BESS/GenSet/RCS/Gateway/OP
Applies to	All MGIS devices
Responsibility	Contractor
Comment	Software engineering practices should assure that invalid input is detected and acted upon in a safe and secure manner.

15.6 Error Handling

15.6.1 The Microgrid information system shall identify error conditions, and generate error messages that provide information necessary for corrective actions without revealing potentially harmful information that could be exploited by adversaries.

Type of control	Capability, Configuration
Where applied	MGC/BESS/GenSet/RCS/Gateway/OP
Applies to	All MGIS devices
Responsibility	Contractor
Comment	The extent to which the Microgrid information system is able to identify and handle error conditions is guided by organizational policy and operational requirements; (2)