OT NETWORK- CYBERSECURITY POLICIES AND PROCEDURES

A. Risk Management Objectives. Cybersecurity threats to Operational Technology systems are increasing dramatically with consequences that impact occupant safety, loss of productivity, equipment damage, tenant satisfaction, and access to business data assets. The cybersecurity policies and procedures contained within this specification are intended to minimize these risks while preparing the organization to manage risk on an ongoing basis including recovering from a disastrous incident.

B. Owner Policies: The following policies are to be finalized and updated with the Owner prior to project completion in conjunction with the MSI. In some cases, the policies apply to post-construction support during and after the warranty period.

1. User Authorization Policy. The MSI is authorized to add, modify and delete users to the Integration Platform subject to compliance with the Owner’s Password, User Removal, and Administrative User policies. In addition, the MSI will submit the results of a six-month User Audit during the warranty period to confirm compliance with these policies.

2. Password Policy. All users are to adhere to the following requirements:

a. Every user is to have a unique username and password.

b. No shared accounts are permitted.

c. Passwords are to be a minimum of 8 ASCII characters in length including spaces. Easy to remember phrases are recommended.

d. Passwords should never be reused.

e. Passwords must be changed on first log-in.

f. This policy applies to both the Integration Platform application and the associated Operating System (OS).

3. User Removal Policy. The MSI will remove access within one business day by their users who are no longer employed or whose job responsibilities have changed such that they no longer require access to the Integration Platform.

4. User Audit Policy. The list of users for the Integration Platform will be audited every 6 months to ensure that only authorized users remain and that their privileges are consistent with the role they perform. Accounts used for normal operations should not be able to perform elevated actions.

5. Administrative Users Policy. The Integration Platform shall have a minimum of 2 System Administrators and a maximum of 4 with at least one of the administrators being an employee of the owner. System administration privileges should be granted to those individuals whose role requires this privilege in order to fully configure and program the system including creating new users.

6. Internet Management. Internet access to the Integration Platform is to be managed to the Owner’s IT department.

7. Backup Policy. The Integration Platform server is to have a system image backup performed by an enterprise grade backup service including daily incremental changes. Backups are to be stored in a secure location with redundancy. Systems capable of backing up downstream devices configurations are to be configured to do so. If critical components such as a database are hosted on a separate server then those services must also be backed up according to this policy. The MSI and Owner will determine at the onset of the project whether backups are to be managed by the Owner or the MSI under a separate service agreement.

8. Integration Platform Server Management Policy. The MSI and Owner will determine at the onset of the project whether management of the Integration Platform server is to be the responsibility of the Owner or the MSI under a separate service agreement. Management of this server includes compliance with the following:

a. The server will be located in a secure environment. This means only intended administrators of the system are to physically access the system. Keyboard, mouse and monitor should not be attached when not in use. Unauthorized users should not be able to plug in any USB device.

b. Anti-virus / anti-malware software will be installed with new signatures and updates applied automatically. Virus updates will be monitored to detect possible negative impacts to the operation of the Integration Server application software.

c. The operating system (OS) software must be running a fully supported version with all security patches installed.

d. The hardware platform will be monitored for processor, memory and storage performance including real-time alerting.

e. The only application software resident on the Integration Platform Server will be the IoT Server Software.

9. Remote Communications Policy. The Integration Platform is not to be publicly accessible over the Internet. Connections are to be made through a VPN or other remote management solution. Refer to the Operational Technology Network section of this specification for details on the remote management solution. Management of the VPN is by the Owner.

10. Disaster Recovery Policy. In the event of a critical failure or breach of the Integration Platform, the Owner and MSI will develop a disaster recovery plan that includes the following topics at a minimum:

a. Backup restore procedure

b. Manual operation

c. Communication plan to internal staff and occupants

d. Failure analysis

C. System Configuration Policies: The Integration Platform will comply with the cybersecurity configuration policies defined in section 2.9.

1. Application Software Policy

2. Password Policy

3. Administrative Users Policy

4. Guest Accounts

5. Manufacturer Default Accounts

6. Auto-lockout Policy

7. Auto-logoff Policy

8. Activity Logging Policy

9. Authentication Encryption

D. Subsystem Configuration Policies: Each of the systems that are to be integrated by the MSI are also to be configured according to the Configuration Policies by their respective Contractor.