SECTION 25 00 00

INTEGRATED AUTOMATION

TABLE OF CONTENTS

SECTION 25 00 00

INTEGRATED AUTOMATION

PART 1 - GENERAL

1.01   GENERAL AND SPECIAL CONDITIONS

A.   The Dartmouth College Design & Construction Guidelines include general administrative, design, product, and installation requirements. It is the intent of Dartmouth College that the consultant incorporates the requirements contained herein with the consultant's specifications to produce a document that is cohesive, coordinated, and non-conflicting. Deviations from these Guidelines must be reviewed and approved by the appropriate DC-FO&M Engineering representative.

B.   System Description:

1.   The purpose of this section is to detail the requirements for integration of applicable project systems, including the lighting controls system, electrical metering, water metering, and thermal utility metering, into the BAS front-end through open industry-standard tools, protocols, and practices to produce a single GUI for control and monitoring.

C.   The requirements of this guideline shall be contracted directly to the Construction Manager and not through the Mechanical Contractor.

D.   The Building Automation System (BAS) contractor shall be responsible for ensuring compliance with this section and Section 23 09 23 – Automatic Temperature Controls.

E.   Drawings and General Provisions of the Contract, including General and Supplementary Conditions Division 1 Guideline, apply to this Section.

F.   This Project will be Commissioned per Guideline 01 91 00 – Commissioning.

1.   Refer to commissioning guidelines for all relevant disciplines for commissioning information and responsibilities.

2.   Commissioning Process: Will require additional labor, material and/or other costs to be provided by the Contractor as part of the Project.

3.   Commissioning Agent: To be contracted directly with the Owner and not through the Contractor.

1.02   REFERENCES AND DEFINITIONS

A.   Active Directory (AD) or Single Sign On (SSO) - Authentication and authorization service for users that will enforce security policies associated with Owner IT secure access requirements.

B.   Automatic Temperature Controls (ATC) contractor – The contractor responsible for the automatic temperature and control systems and equipment.

C.   BACnet - The open ASHRAE/ANSI communication protocol, Standard 135 that allows open communication between building systems and devices.

D. Building Automation System (BAS) - The building controls involved with the operation of all HVAC systems.

E. Building Automation System Contractor (BAS Contractor) – is the contractor that furnishes, installs and integrates the Building Automation System.

F. Building Automation System Controllers (BAS controllers) - field programmable, microprocessor-based type incorporating direct digital control and energy management functions; same as a field controller NIA or NAC.

G. BAS Licensing - Dartmouth college is the listed owner on all software licenses and toolkits associated with BAS programming.

H. Dartmouth College Controls Vendor Standards for Building Controls Project Documentation and Software Control are minimum requirements for all controls vendors. Reference Appendix B.

I. Edge device – is any device installed in a "Field Setting" that is incorporated into a larger system and intended to provide real-time data and/or control. Edge devices are most commonly IP-network connected and provide connectivity between local building networks and wide area networks.

J. FDD – Fault Detection and Diagnostics is the enhanced analytics system and process that qualifies and quantifies building system information from alarms and alerts into standardized and user-identified categories to efficiently address and resolve building and operational problems.

K. Field controller – is a programmable microprocessor-based device that directly operates field mechanical or electrical equipment using two-way communication.

L. GUI - Graphical User Interface. This is an operational control and monitoring dashboard from which all system and subsystems can be accessed through a single, browser-based system, or "Unified User Interface" (UUI).

M. HVAC - Heating Ventilation and Air Conditioning.

N. Information and Communication Technology Platform consists of network communications infrastructure (wired and wireless) and hosting systems for applications required for the Smart Building Platform that confirms to all Dartmouth Information Security (DISC) Policies.

O. IoT Devices – "Internet of Things" or Edge devices connected to Dartmouth's Operational Technologies network that directly interact in real-time with one another, share data, and allow an action, command, or input from one system or device to produce a response, output, or sequence to another system or device.

P. Machine User Account – A User Account profile intended to allow one system to communicate and transmit information between another system through the access control of a username and password dedicated to the non-human user. This typically used for automated tasks and transactions such as a weather station feed. Machine user accounts do not time out.

Q. M&M – The Measurement & Monitoring Plan describes the criteria established by the Owner for the continuous monitoring of equipment, energy, gas, and water usage.

R. NAC - Network Access Controller is a field device intended for integration between Owner

network and BAS field control devices. The NAC provides global supervisory function and control over lower-level controllers in integrated sequences. The NAC operates as a protocol converter for multiple protocols communicating on both serial and IP.

S.   Networks – Dartmouth operates its own converged networks.

T.   NIA – Network Integration Appliance is the interface between the building's communications system and the BAS control devices.

U.   Open licensed/sourced – Any control device, field controller, NAC, or Server-based platform operating on a license that is "unrestricted" and lists the Owner as the "Named License Holder". This software licensing model ensures ownership of all equipment, software, configurations, data files, code, and documentation associated with the Owner's systems. Any qualified vendor can work on open licensed systems provided they have access to the required BAS system toolkits.

V.   Open protocol – is an industry-accepted Network Standard that is an established set of rules that determine how data is transmitted between different manufacturer's devices on the network (i.e. TCP/IP, Modbus, LonTalk, etc.)

W.   OT – Operational Technology includes the hardware and software for monitoring, control, data analytics and visualization for lighting, energy, mechanical systems, security, elevators, space utilization, traffic, transportation, and parking.

X.   RAID – Redundant Array of Independent Disks

Y.   REST – Representational State Transfer

Z.   Smart Building Platform (SBP) – The integrated platform that entails all controlled and monitored building systems and infrastructure including hardware and software for disparate systems. Currently this platform is the same as the BAS front-end platform.

AA. Sub-points – Sub-points are points associated with packaged controls.

BB. Terminal Unit Controller – any controller for thermal equipment, i.e. VAV boxes, Fan Coil Units, Cabinet/Unit Heaters, Radiators, etc.

CC. User Accounts – User accounts are in this context human accounts and not "machine user accounts".

DD. VFD - Variable Frequency Drive

1.03   SCOPE OF WORK

A.   The BAS Contractor is responsible for producing a fully functioning BAS in each facility including installing new controls, configuring existing controllers for open and unrestricted communication (as applicable), and commissioning the mechanical BAS. Refer to the Guideline 23 09 23 - Automatic Temperature Controls.

B.   The BAS contractor shall integrate all metering and lighting controls devices exposed by the lighting contractor for integration into the SBP for read-write capability. Future capabilities to incorporate an analytic engine for Fault Detection and Diagnostics (FDD).

1.   SBP Basis of Design

a. Open-licensed, open-protocol building systems.

b. The SBP shall have the capability to integrate any point from:

    1)   Automatic Temperature Control system

    2)   Lighting Controls system

    3)   Electric Metering and sub-metering

    4)   Water sub-metering

    5)   Thermal utility metering and sub-metering

    6)   Other devices (i.e. IoT) as defined
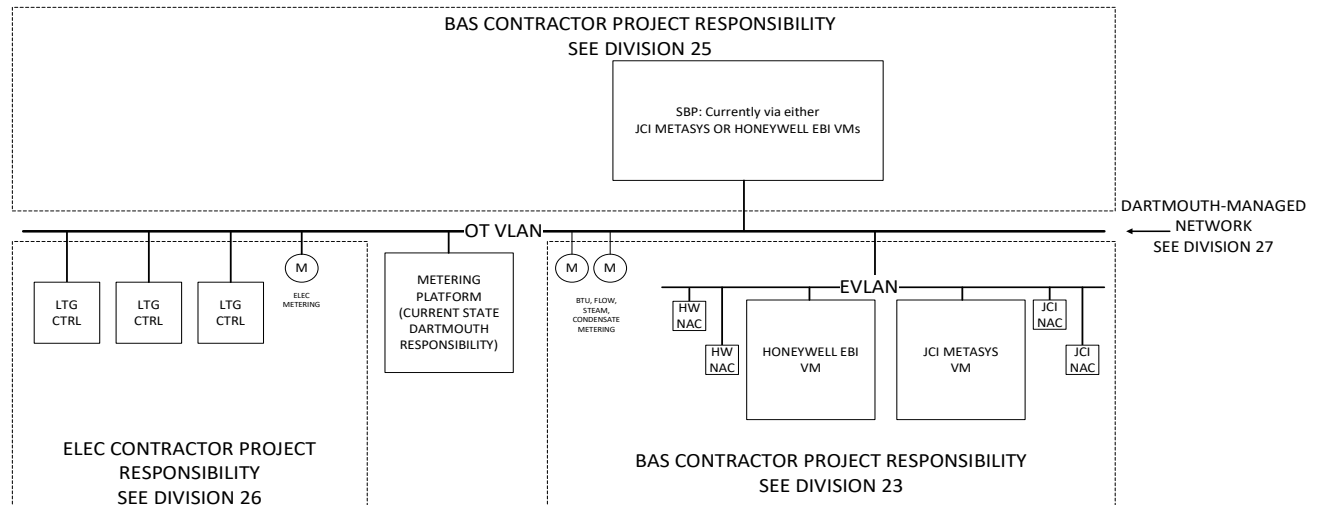
C. All Platform points shall include metadata tagging in accordance with common, industry-accepted metadata tagging schemes. The SBP shall be able to accept either, or both, Brick Schema and Project Haystack tagging Conventions. The Owner shall develop a naming standard for BAS, lighting, and other system implementations that shall not conflict with tagging schemes. Review and coordinate with Dartmouth College for metadata tagging schemes.

D. The building sub-systems shall be capable of exchanging data as defined in other divisions or provided as part of the project and shall include but not be limited to the referenced guidelines below.

E. The BAS contractor shall work with the Owner's IT group to further develop cybersecurity policies and procedures for this implementation.

1.04   RELATED REQUIREMENTS

A. See Appendix A for Division 25 related Coordination Matrix for Building Automation Systems (BAS).

B. Requirements of Division 25 Guidelines also apply to the following sub-systems:

1. 23 05 19 - Meters and Gauges for HVAC Equipment
2. 23 05 20 - Thermal Utility Meters
3. 26 09 43 - Lighting Controls
4. 23 09 23 - Automatic Temperature Controls
5. 26 16 00 - Electric Metering
6. Dartmouth Information Security Policy
   https://policies.dartmouth.edu/policy/dartmouth-information-security-policy
7. Division 27 Telecommunication Master Construction Specifications, Guidelines, and Reference Designs https://sites.dartmouth.edu/networkservices/specs/.

C. Open Communications Protocol:

1. The sub-system(s) contained in the above divisions and sections shall provide open protocol communications hardware and software <u>based on IP-based connectivity</u> utilizing TCP/IP, ASHRAE BACnet I/P and BACnet MS/TP, Modbus RTU, Modbus TCP, MQTT, OPC UA, SOAP and SNMP or protocols with open communications such as REST API standards of data exchange.

   a. IP-based communications are the preferred communications protocol for Integrated Equipment. Serial communications that are approved include: BACnet MS/TP and Modbus RTU. Appropriate uses of serial communications are as outlined below:

      1) Terminal units that are installed onto existing serial trunks may use serial protocols.

      2) Serial-based metering equipment that does not support native IP-based protocols. These devices shall be routed to a Dartmouth-approved Serial-to-IP gateway.

      3) Old and currently-installed VFD's that operate on serial trunks.

      4) Isolated equipment that requires distances exceeding 300 feet, but not over 4,000 feet.

   b. Modules that are used to create interactive applications and analysis applications may include.
      1) Real-time data services, which are used to create applications to integrate third-party hardware or systems. REST API, used to create HTML pages that contain data sourced from the server.
      2) Open Protocol Industry standards including LonMarks, BacNet, Modbus, OPC(OLE), AdvanceDDE and ODBC

   c. For all current field devices communicating via serial protocol, coordinate the installation of a serial-to-IP converter adjacent to the serial device or serial trunk head-end device. Coordinate with Dartmouth Network Services for nearest IP-demark. Serial trunks shall be segmented and separated by end-device manufacturer and protocol. Do not mix manufacturers on the same trunk. Serial trunks communicating between VFD loads shall be separate from all other non-VFD trunks.

2. The vendors and contractors for the referenced sub-systems shall program the databases to comply with data exchange rules for the listed protocols including but not limited to all physical, virtual and calculated points, and operating parameters for their respective system.

   a. In a future state, all setpoints, schedules, overrides, alarm functions, and any data value within the entire system architecture shall provide read/write access to the SBP.

3. The BAS contractor and each sub-system contractor shall coordinate with Dartmouth College BAS Control Shop and Campus Services Technology Services (CSTS) regarding network addressing and database exchange. This must include the timing sequence for the

updates of the data exchange between the systems and the validation that all subsystem data values are available for commissioning prior to project turnover.

1.05   ROLES AND RESPONSIBILITIES

A.   See Appendix A Coordination Matrix for Building Automation System (BAS).

B.   The BAS-Contractor shall be responsible for integrating all BAS, electric, water and steam metering, and lighting controls points into the SBP.

C.   The Owner shall direct all network coordination and configuration for authentication. It is the responsibility of the BAS Contractor to understand and adhere to all Dartmouth IT requirements.

D.   All contractor's submittals for the sub-systems contained in the above divisions and section shall be reviewed by the BAS Contractor to assure completeness and data exchange conformance for complete functionality defined herein.

E.   The use of any portion of the IT infrastructure by any building sub-system must meet the Owner's IT standards and policies. It is the responsibility of the BAS Contractor to acquire and understand the Owner's IT standards for cloud services, servers, network storage, network appliances, databases, routers, switches, and any other software or hardware.

F.   The BAS Contractor shall be responsible for all BAS and DDC-level controllers (both new and existing, and both serial and IP-based controls), control devices, control panels, controller programming, controller programming software, controller input/output and power wiring and controller network wiring. The BAS contractor is responsible for programming all mechanical Sequences of Operations (SOO's).

G.   The BAS Contractor shall coordinate the IT requirements for the server(s), Network Integration Appliance(s), and all other hardware and software required for a complete SBP.

H.   All contractors installing metering, BAS equipment and lighting controls, shall complete an integration checklist and submit to the BAS Contractor prior to construction.

I.   The BAS Contractor shall be responsible for assisting the Commissioning Authority to commission the integrations between systems.

J.   The BAS Contractor shall coordinate the requirements and installation of all network switches, port requirements, and locations required for full SBP integration with the Owner. Reference Owner Network requirements and guidelines.

K.   All IP-based cabling between Dartmouth network switches and the demark location of the BAS, lighting, and metering system controllers is the responsibility of the Division 27 contractor. All IP cabling between controllers and the demark is the responsibility of the BAS or electrical contractor.

L.   The Division 26 lighting controls contractor shall be responsible for the complete installation, Sequences Of Operation (SOOs), programming, and exposing all BACnet points for read/write or integration through open protocols.

M.   The BAS Contractor shall integrate the Division 26 systems as supplied by the Division 26 contractors as required to enable ATC sequences of operation. Lighting control points shall be visualized for command and control using tabular graphics including floorplan graphics.

N.   The Division 26 contractors shall be responsible for the location, powering, and installation of all electricity metering and submetering equipment, including panels, enclosures, conduit, power wiring, terminations, and the identification of all communication protocols and mapping to provide to the BAS Contractor.

O.   Only contractors that are pre-approved by Dartmouth College Network Services may install, connect, or service network equipment or cables that are intended to interoperate with the campus Network.

P.   Network Jacks and/or other telecommunications demarcation points must be coordinated with and appear on the Telecommunications set of drawings for the project. Network Jacks that are not properly indicated on the Telecommunications Construction Drawings may not be installed or activated.

Q.   The BAS Contractor shall integrate all metering into the SBP. The BAS Contractor shall confirm with the Division 22, 23 and 26 contractors that all metering is configured, programmed for the intended application, and functions as designed.

R.   The BAS Contractor shall be responsible for implementing Owner Network and Security policies and procedures affecting the SBP

S.   All contractor's submittals for the sub-systems contained in the above divisions and section shall be reviewed by the BAS contractor to assure completeness and data exchange conformance for complete functionality defined herein.

1.06   QUALITY ASSURANCE

A.   Codes and Standards:

North American Standards:

1.   UL Compliance: Provide electrical components of Division 25 control systems which have been UL-listed and labeled and comply with NEMA standards. Provide control devices, which are UL listed as a signal appliance.
2.   Comply with NEMA standards pertaining to components and devices for Division 25 control systems.
3.   NFPA Compliance:

    a.   NFPA 90A "Standard for the Installation of Air Conditioning and Ventilating Systems" (Where applicable to control systems and control sequences).

    b.   NFPA 72 "National Fire Alarm and Signaling Code"

4.   National Electric Code (NEC)
5.   National Electrical Safety Code (NESC)
6.   American National Standards Institute (ANSI)
7.   American Society for Testing and Materials (ASTM)
8.   Occupational Safety and Health Association (OSHA)
9.   Institute of Electrical and Electronics Engineers (IEEE)
10.   Any other applicable Federal, State, Provincial and/or Local Codes
11.   ASHRAE Standards current edition.
12.   National Institute of Standards and Technology (NIST)

B.   Materials and equipment shall be the cataloged products of the manufacturers regularly engaged in the production, development, and installation of defined Division 25 systems. The BAS contractor shall ensure that all materials and equipment are the manufacturer's latest standard design and comply with Division 25 requirements.

C.   Radio Frequency: All electronic equipment shall conform to the requirements of FCC Regulation, Part 15, Section 15, "Governing Radio Frequency Electromagnetic Interference," and be labeled accordingly.

D.   Refer to Section 33 83 00 – Wireless Communications Transmission and Distribution, https://dartgo.org/DartmouthNetworkMasterSpec and confirm with Owner for location and application of wireless sensor prior to installation.

E.   Performance Standards:

   1.   Systems shall be tested using manufacturer's recommended hardware and software for operator workstation as a minimum (server and browser for web- based systems).
   2.   Systems shall conform to the following minimum standards over network connections:

      a.   Graphic Display: Animated graphics with 20 dynamic points shall display the most current data with a response time of fewer than 5 seconds.

      b.   Graphic Refresh: A field-based data graphics with 20 dynamic points shall update with the most current data with a response time less than 8 seconds and shall automatically refresh with a response time less than 5 seconds.

      c.   Configuration Screens: Screens used for configuration, calibration, optimization, PID loops, and similar control logic shall automatically refresh within 6 seconds.

      d.   Object Command: Devices shall react to command of a binary object within 2 seconds. Devices shall react to command of an analog object within 2 seconds.

      e.   Alarm Response Time: An object that goes into alarm shall be annunciated at the workstation within 15 seconds.

      f.   Program Execution Frequency: All custom and standard applications shall be capable of running as often as once every 5 seconds. Execution times should be selected to be consistent and applicable to the mechanical process(es) under control.

      g.   Performance: Programmable controllers shall be able to completely execute DDC PID control loops at a frequency adjustable down to once per second. Select execution times consistent with and applicable to the mechanical process(es) under control.

      h.   Multiple Alarm Annunciation: Each workstation on the network shall receive alarms within 5 seconds of the other workstations on the same network.

F.   The BAS contractor must comply with the "Dartmouth College Controls Vendor Standards for Building Controls, Project Documentation and Software Control". See Appendix B of this guideline.

1.07 **SOFTWARE LICENSING**

A. The Owner shall be the named license holder of all BAS, lighting, and metering and SBP software. In addition, the Owner shall retain ownership of all project-specific configuration documentation, data files, and application-level software developed. This shall include all custom, project-specific software code and documentation for all configuration and programming that is generated. This is to include all code and documentation configured for use with the BAS, lighting controls, metering, SBP, NIA's, and other related communications devices. Required usernames and passwords for access to any component or software program shall be provided to the Owner upon SBP project closeout as well as during SBP construction.

B. Any annual license fees or data subscription services shall be included for the first year of operation, starting at the installation of the device or software for programming. Additionally, the annual fee for subsequent years should be outlined in the proposal over the lifecycle of the respective product.

1.08 **SUBMITTALS**

A. Submittals:

1. Submittals are required for all equipment prior to ordering or fabrication of any system or subsystem. No deviations from the submittals, as originally approved, shall be permitted. Any materials purchased prior to approval shall be at the sole risk of the <u>applicable sub-system contractor</u>.
2. All documentation shall include a table of contents that is well organized, indexed, and tabbed with reference to the specific section (also sub-section if applicable) of the guideline. If catalog cut sheets or published materials include information that is not applicable to the item furnished, the applicable sub-system contractor shall clearly indicate what information is applicable and clearly notate accordingly. Indicate all options and/or accessories to be specified with the device when ordered. Indicate complete part numbers to be ordered with all options called out specifically.
3. Administrative Data: Submit the name, address, and telephone number of the local service representative. A guarantee is required that the applicable sub-system contractor will provide a maximum of a 24-hour window for onsite response to trouble calls, applicable 24-hours a day, during the warranty period.
4. Identification and Labeling: For all category cabling, refer to Division 27 for requirements.
5. Submit the following for each sub-system:

    a. Integration Hardware

        1) A complete bill of materials indicating quantity, manufacturer, model number, and relevant technical data of equipment to be used.

        2) Manufacturer's description and technical data such as specifications, cut sheets, installation instructions, and operation/maintenance manuals for items listed below as well as for relevant items that are not listed below but are pertinent to the system:

            a) Database Requirements (physical or virtual machines, Cloud services)

            b) Server Requirements (physical or virtual machine services or Cloud services)

      c)   Network Integration Appliance Requirements

      d)   Control Panels

      e)   Power Supplies

      f)   Uninterruptible Power Supplies (UPS)

      g)   Operator Interface Equipment

      h)   Wiring (Power and Communications)

3) Device hardening and data encryption methodology (cyber security) Provide documentation for the classification of data. Wiring diagrams and layouts for each respective control panel. Show all termination numbers, and detail pinouts when the termination is non- standard.

4) Floor plan schematic diagrams indicating all Platform and subsystem equipment locations.

5) Riser diagrams showing control network layout, communication protocol, and wire types.

b. Controlled Systems - Verify with Division 23 – Automatic Temperature Controls (BAS Controls) Contractor and Division 26 (Electrical) Lighting Controls Contractor that the following is accessible and reflects current-state conditions:

1) Riser diagrams showing control network layout, communication protocol(s), and wire types.

2) Schematic diagram detail of each controlled system.

3) A complete bill of materials for each controlled system.

4) BAS & Lighting Controls O&M Manual: Complete narrative description of control system operation, including sequences of operation. Include and reference the schematic diagram of the controlled system. List all hardware and software I/O points that are required to operate the systems as well as indicate which points are alarmed and/or trended points.

5) Future FDD System: Complete description of user guides, configuration manual, gateway installations, security and IT guides, and FDD rule reference guide including fault description, system assignments, and point requirements.

c. Description and approval of the testing process(es), any checklists, and report formats to be used for functional testing, validation, and certification during the commissioning phase.

d. BACnet Protocol Implementation Conformance Statement (PICS) for each submitted type of controller and operator interface.

    e.   https://www.bacnetlabs.org/page/BTL_Cert_Program Modbus register and tables, https://modbus.org/certification.php, Submit results from Modbus conformance test.

    f.   Elevations and other applicable details as required to effectively depict the system.

    g.   Coordinate with Division 22, 23, 26, 27, 28 and 33 contractors to obtain, document, and submit a list of all devices and systems, including a list of "sub-points" available from each device and system. Describe what specific "sub-point" parameters are available, if they are available for viewing only, and if they are capable of being modified from a workstation. Indicate which "sub-points" are being integrated as part of the document requirements and what their functions are. Also, detail the "sub-points," if any, that cannot be integrated and explain. The Owner shall select which additional "sub-points" are to be integrated, if any, and what their functions shall be. Include all integrated "sub-points" in the Point List submittal described below. The BAS contractor shall provide drafts of integration checklists (see Appendix D for example integration checklist) for both the owner and the engineer as a review for subsystems. This document, at a minimum, should identify the following:

        1)   Type of device to be integrated

        2)   Selected protocol for system or subsystem

        3)   System/subsystem location

        4)   Addresses (both IP and MAC) and Instance IDs in MS Excel format.

        5)   Equipment information including make/model/revision/serial number

        6)   System architecture: provide a drawing of the proposed system architecture showing configuration and locations for the Server(s), controllers, terminal unit controllers, system servers, IoT devices, gateways, control wiring for each device, any hardware/wiring/terminations for connections. Indicate the spare capacity and BACnet instance number or network address for each device. Include approved networking hardware such as switches, converters, routers, broadcast management devices, applicable cabling, and applicable terminations. Also, provide IP addresses and VLAN segments, TCP and/or UDP port numbers, and firewall rules (where applicable). Provide diagrams of the proposed control power infrastructure to include: the designation of the electrical panelboards that will be utilized to provide control power, the quantity/configuration/size/location of control system transformers, and the wiring to distributed control devices that require power.

    h.   Provide floor plans showing equipment locations that have been coordinated with the work of other trades for areas within the project's scope.

    i.   Shop Drawings: Submit all drawings required for the construction, commissioning, maintenance, and future expansion of the system in addition to the subcontractor drawings. The title block shall bear the names and signatures of

r.   Provide a set of building floor plans showing the location of all points, controllers, and electrical panels used for power sources. The Mechanical CAD/Revit drawings should be used for this reference set. All points should then be represented with a symbol at the point location coupled with the point name and descriptor next to the symbol.

s.   Customized Graphics Samples: sample equipment graphics should include but not be limited to sample floor plans, AHUs, chilled water and heated water systems (where applicable), zone terminal units, exhaust fans, Dedicated Outdoor Air System (DOAS) units, metering dashboard, and generators.

t.   Product Data: Submit technical product specification sheets for each system component and device, which includes all data needed to prove compliance with this guideline. Clearly indicate the exact model of each component to be provided along with the associated accessories or options required.

u.   Manufacturer's Installation Instructions: Submit for all components being provided under this section.

v.   Schedules: schedule of work provided within one month of contract award, indicating:

   1)   Submittal schedule and approval timeline requirements.

   2)   Intended sequence of work items.

   3)   Start date of each work item.

   4)   Duration of each work item.

   5)   Planned delivery dates for ordered material and equipment and expected lead times.

   6)   Milestones indicating possible constraints to work by other trades or situations.

   7)   Weekly written status reports shall be provided, indicating work completed and any revisions to expected delivery dates. Include updated schedule of work with each status report.

B.   Pre-Commissioning Submittals:

   1.   Operator's and programmer's manuals: Submit for all operating, user, and application software provided, including all platform and third-party software furnished.

C.   Project-Specific Submittals: Submit a representative sample, for each of the following, prior to final development of each for the entire project. Once the Owner's approval has been obtained for the representative samples, complete submittals for the entire project are to be provided.

   1.   System Object Groups: Include printed copies of all System Object Groups developed for this project.

2.   Input/output Object Testing: Include copies of all Testing Documentation Forms required to be completed for this project. At a minimum, the following must be included (as applicable): hardware address, object name, device type, transmitter type, signal range, signal formula, and readout formula.

3.   Software Documentation: Submit input/output point name definitions, data object name definitions, a complete listing of control routine file names, a printed copy of each control routine, a narrative description of each control routine's function in English, and a printed copy of each system grouping and graphic display for this project.

4.   Sequence of Operation Testing: Submit a copy of the Sequence of Operation annotated with the Subcontractor's testing methods. Proposed methods will be performed to prove compliance with the project specification.

D.   Project Record Documents: Submit (as-built) documents upon completion of installation for approval prior to final completion. Submittal shall consist of:

1.   Project Record Drawings: Digital As-built versions of submittal shop drawings will be provided as editable AutoCAD, or Visio compatible files, including 6 prints of each drawing on 11" x 17" paper. All record drawings will be placed on Owner's approved background.

E.   Testing and Commissioning Reports and Checklists: Completed versions of all reports, checklists, and trend logs.

F.   Operation and Maintenance (O&M) Manual: one electronic copy of the following:

1.   Completed as-built versions of submittal product data.

2.   Names, addresses, and telephone numbers of installing contractors and service representatives for the respective equipment and control systems.

3.   Operator's manual with procedures for operating control systems: logging on and off, handling alarms, producing point reports, trending data, overriding computer control, and changing setpoints and variables.

4.   Programming manual or set of manuals with description of programming language and syntax, of statements for algorithms and calculations used, of point database creation and modification, of program creation and modification, and of editor use.

5.   Engineering, installation, and maintenance manual or set of manuals that explain how to design and install new points, panels, and other hardware; how to debug hardware problems; and how to repair or replace hardware.

6.   Documentation of programs created using custom programming language, including setpoints, tuning parameters, and object database. Electronic copies of programs shall meet this requirement if control logic, setpoints, tuning parameters, and objects can be viewed using furnished programming tools.

7.   Digital copies of Graphic files, programs, and databases.

8.   Complete original-issue documentation, installation, and maintenance information for furnished third-party hardware, including computer equipment and sensors.

9.   Complete licensed to owner, original-issue software, including operating systems, custom programming language, operator workstation or web server software, and graphics software.

10.   Licenses, guarantees, and warranty documents for equipment and systems.

11.   Full as-built digital set (PDF format) of system drawings, details, and sequence of operations in half-size ARCH E1 or larger. PDFs shall be clear, legible, and clean of any revision clouds, red-lines, and handwritten notes or mark-ups. This shall include all

drawing references to systems and subsystems from individual low-voltage, controls, electrical, and lighting contractors and subcontractors.

12. Warranty requirements must be defined for each project component including software, hardware, and licenses with defined timelines for warranty start-date and duration.

13. Copies of all training documents, curriculum, presentations, video training sessions. A log of all Owner employees, contractors, and any others in attendance for training sessions.

G. Documentation of Changes During Warranty Period:

1. During the warranty period, all copies of drawing packages and manuals shall be updated to include all hardware and software changes required to resolve issues that are covered by the warranty. Complete digital backups shall be provided at the end of the warranty period and made available to the owner to be stored in their environment to support disaster recovery/business continuity requirements.

H. Training Materials: Provide course outline and materials for each class at least two weeks before first scheduled class. Training to be done in 2 separate sessions. Training shall be in the form of instructor-led sessions, computer-based training, and/or web-based training. Owner will modify course outlines and materials to meet Owner's needs, if necessary. The Owner will review and approve course schedules, outlines, and materials at least three weeks before first scheduled class.

I. Coordination Workshops:

Coordination workshops shall include, at a minimum, the following three session types listed below. The BAS Contractor shall provision for as many workshops as are deemed necessary by the Owner to address all facets of Platform component configuration.

1. Network configuration workshop

   a. The BAS Contractor shall conduct a network configuration workshop with the Owner's IT group for establishing the network and cybersecurity parameters for the project. The ongoing network requirements and documentation shall be established during the workshop and presented as a submittal for approval following the meetings.

2. Graphics workshop

   a. The BAS Contractor shall conduct a graphics workshop with the Owner's Operations group, design team, and commissioning agent for establishing the graphics package for the project. The final graphics workshop shall be a live graphics review meeting.

PART 2 - PRODUCTS

2.01   GENERAL REQUIREMENTS

A. The Small Building Platform (SBP) subsystems:

1. All SBP subsystems shall communicate with the SBP using the ASHRAE 135-2016 Protocol BACnet/IP and/or BACnet/SC (SC where applicable).

2. All SBP subsystems shall have the capability to integrate ASHRAE 135-2012 BACnet and

MODBUS (as well as other open and proprietary communication protocols) to enable one open and interoperable system.

3. Use the newest generation and current products that the manufacturer is currently producing and selling for use in new installations. Do not use this installation as a product test site. Spare or replacement parts and software support shall be available for at least a five-year period from the completion of this contract.

4. Software maintenance agreements shall at minimum be active during implementation and be in force during the warranty period after owner's sign off of the project. Ongoing OpEx costs shall be provided to the owner for future software licensing and SMA's required to allow for security patch management and system enhancements.

5. All devices that communicate via Modbus protocol must provide all protocol and register mapping to the BAS Contractor and Owner.

6. SBP Subsystems which use proprietary communication protocols, mapping, data encoding, or socket types for communication with the SBP are prohibited such as (JCI N2, Honeywell SYLK, Niagara Fox, etc.). If multiple disparate systems require access to the meter data, the applicable subsystem contractor shall provision for multiple communication outputs when ordering meters, prior to construction submittals.

B. Lighting Controls Systems to be integrated:

1. Reference 26 09 23 - Lighting Controls for approved manufacturers

C. BAS Controls Systems to be integrated:

1.   Reference 23 09 23 - Automatic Temperature Controls

D. Meters & Submeters:

1. Electric: Reference 26 16 00 - Electric Metering
2. Thermal Meters, Water Meters and Submeters: Reference Division 23 05 20 - Thermal Utility Meters and 23 05 19 - Meters and Gauges for HVAC Equipment.

E. Variable Frequency Drives: Coordinate this with Dartmouth's Guideline 26 29 00 Low-Voltage Controllers.

F. Network Preferred Manufacturers: Refer to Dartmouth College Guidelines Division 27.

G. Servers - Provided by the Owner. Operating platform must support current, non-deprecated, non-EoL, non-end-of-sale operating systems and databases.

1. Preferred Manufacturers: coordinate with ITC
2. Server configuration for redundancy is Active-Active or Active-Passive depending on vendor support.
3. Preferred hosted server environments include: AWS

H. UPS

1. Higher Level Network Integration Appliances (NIA's) or other field-servers as required: Power through a minimum 15-minute UPS. Consult with DC-FO&M during design to determine the controller level requiring UPS service.

I.   Communications

    1.   Refer to Dartmouth College Guidelines Division 27.
    2.   All controllers and other devices that are intended for integration shall be connected to the Owner's OT LAN.
    3.   The only accepted non-IP communication protocols for NIA's shall be Modbus RTU and BACnet MS/TP.
    4.   Coordinate with the Owner for network interface requirements. Provide a network interface to the server.
    5.   Local connections shall be via the Owner's OT LAN on a dedicated VLAN.

PART 3 - EXECUTION

3.01   INTEGRATION

A.   The <u>BAS Contractor</u> shall integrate all ATC controls points, lighting points and meters as specified for the project.

B.   Provisioning of Backups

    1.   <u>The BAS Contractor</u> shall coordinate and document the backup policies for the following devices:

       a.   Servers

       b.   Databases

       c.   Connected Devices including:

          1)   Network Area Controllers

          2)   Network Integration Appliances

          3)   Controls integrator Equipment Including

             a)   All Field Device Controllers (AHU's, TU's, etc.)

    2.   Coordinate with Dartmouth IT for approved backup or off-site storage for all backups.
    3.   Coordinate the automation and frequency for all backups.

C.   Lighting

    1.   The lighting control systems are defined in Guideline 26 09 23 Lighting Controls.
    2.   The BAS contractor shall coordinate and subcontract if necessary to RFI and receive integration information from the lighting controls manufacturer if the initial as-built documents for lighting controls are not readily available from the Owner.
    3.   The BAS contractor and lighting controls installer shall coordinate communication requirements.
    4.   All occupancy sensors for the lighting control system shall be integrated such that the BACnet objects are available for HVAC control sequences.

D. BAS and ATC controls are installed by the BAS Contractor and defined in Guideline 23 09 23 – Automatic Temperature Controls.

1. The BAS equipment and systems shall be integrated into the SBP for all future monitoring and FDD requirements.

E. Metering and sub-metering

1. The BAS contractor shall integrate all meters and submeters for electricity, thermal utility, and domestic water into the SBP to collect all point data required for monitoring and future FDD.

3.02 INSTALLATION

A. The NIA installations shall have sufficient spare capacity for spare DIN-rail mountable modules to accommodate future-state required points for integration including hardwired and serial communication. Enclosure shall provision for enough spare capacity volume to expand up to 300% of existing NIA form factor.

B. The BAS Contractor shall furnish on-the-job supervision for the proper installation of devices in cooperation with, or as may be required by, other trades. This supervision shall include the following:

1. Attend GC, Owner, and hosted meetings in order to disseminate pertinent information and action items to the respective trades.
2. Provide specific on-site instructions to others on mounting and installation to assure that the installer is properly instructed in the work.
3. Provide supervision as required by others to properly perform installation work.
4. Install, test, troubleshoot and correct all system software provided under this guideline.
5. Provide all addresses (both IP and MAC) and Instance IDs in MS Excel format.

C. The BAS Contractor shall furnish all material and labor to provide a complete and functional system, which operates in accordance with the requirements of this guideline.

D. The BAS Contractor shall provide all documentation and sequencing for complete SBP Disaster Recovery that documents all programs, files, links, and drive locations of regular backups necessary for complete replacement of the SBP subsystem and Servers in the event of catastrophic failure.

E. The BAS Contractor must verify IP network connectivity and sub-system connectivity schedule is coordinated with the Owner IT Team for the timely installation of the server and the software.

F. The BAS Contractor is responsible for delivering the SBP subsystem hardware to the installation site, unloading, and securing the hardware.

G. The BAS Contractor shall ensure that all components defined or required to complete the installation satisfactorily are included, are compatible with each other, and are compatible with the conditions of installation and expected use.

H. The BAS Contractor shall ensure the overall effective integration and correctness of individual

parts and of the whole system.

    1.   Upon discovery of a deficiency inherent in any sub-system, BAS, Lighting Controls, or metering, the BAS contractor shall notify Dartmouth:

        a. Indicate the deficiency in a master deficiency log.

        b. Inform Dartmouth of the impact of the deficiency on the overall integration.

        c. Offer consulting or engineering services or strategy intended to resolve the deficiency.

            1) Add scope services to consult to Dartmouth, BAS and lighting contractors, consultants, or any other contractors required to resolve the deficiency.

    2.   BAS contractor shall act as project manager over all sub-system manufacturers. Project management practices and procedures must comply with Dartmouth standards for campus project management. Reference https://www.dartmouth.edu/fom/services/project_mngmt_services/

I.   Provide a designated project manager who shall be responsible for the following:

    1.   Construct and maintain the project schedule.
    2.   On-site coordination with all applicable trades and subcontractors.
    3.   Authorized to accept and execute order and instructions from Owner/Architect
    4.   Single point of contact.

J.   Site and Schedule Coordination:

    1.   The BAS Contractor shall coordinate and schedule work with other work in the same area and with work dependent upon other work to facilitate mutual progress.
    2.   The BAS Contractor shall integrate all facets of the integrated systems installation into the project construction schedule.
    3.   The BAS Contractor shall coordinate schedule updates and changes with the various integration manufacturers.

3.03   COMMISSIONING

A.   Upon completion, the BAS Contractor shall start up the system and perform all necessary debugging operations.

B.   The BAS Contractor shall confirm that all contractors and subcontractors have verified that all hardware components are installed, connected, communicating, and operating properly.

C.   Verify that all systems are operable from local controls in the defined failure mode upon panel failure or loss of power. These procedures shall apply to all gateways to other systems.

D.   Verify that all system software is installed, configured, and complies with defined functional requirements.

E.   Verify that all graphics operate and respond based on performance requirements.

F.   Perform final acceptance testing in the presence of the Owner's Representative and Engineer,

executing a point-by-point inspection against a documented test plan that demonstrates compliance with system requirements as designed and defined.

G.   Conduct final acceptance testing in the presence of the Owner's Representative, and Engineer, verifying that each device point, and sequence is operating properly and reporting.

H.   Acceptance test is contingent on successful completion of check-off. If check-off is not completed due to additional work required, the test shall be rescheduled, and another complete check-off shall be conducted until complete in one pass, unless portions of the system can be verified as not adversely affected by additional work.

I.   System shall not be considered accepted until all acceptable test items have been successfully checked off and accepted in writing. Beneficial use of part or all of the system shall not be considered as acceptance of the system.

J.   Commissioning Agent shall scan network using Wire-shark and Optigo VisualBACnet (or equivalent) and produce a network diagnostic report with recommendations for improvement, if required.

K.   This section is to be coordinated with the Commissioning Agent Contractual Agreement and responsibilities per Dartmouth College requirements.

3.04   TRAINING

A.   Training

1.   Provide training of the building's personnel in the proper operating procedures. The O&M manuals shall be used and referenced as part of the training program. All training sessions shall be recorded with video files made available to the owner for future training.

2.   The <u>BAS Contractor</u> shall provide 24 hours of instruction to the Owner's designated personnel on the operation of the Platform. Operator training shall include, but not be limited to the overall operation program, equipment functions (both individually and as part of the total integrated system), commands, systems generation, advisories, and appropriate operator intervention required in responding to the system's operation.

3.   The training shall be in 6 sessions as follows:

a.   Initial Training: Three one-day session (8 hours) to accommodate multiple shifts for the 24 hour operations of the site after the system is started up and at least one week before the acceptance test. Topics covered include:

1)   Owner application access.

2)   Assigning appropriate access rule.

3)   System logging.

4)   Platform site navigation.

5)   GUI (Graphical User Interface) - How to interact through a web browser.

6)   How to create a trending/history chart builder file.

7) How to export history/trending data.

8) Scheduling of the equipment and lighting control

9) TLS CERT installation.

10) Provisioning for backups.

4. Follow-up Training: Three two-day sessions (16 hours) after the system has been accepted. These sessions shall deal with more advanced topics as requested by the Owner, such as how to add additional points, create and gather data for trends.

5. Training session material, dates, and attendees shall be logged for later reference. Both BAS contractor and all individual users trained shall provide final sign-off confirming proficiency.

END OF SECTION

Appendix A: Coordination Matrix for Building Automation Systems (BAS)

COORDINATION MATRIX				
Work	*Furnish*	*Install*	*Low Volt, Wiring/Tube*	*Line Power*
BMS low voltage and communication wiring (see Note 1 below)	BAS	BAS	BAS	BAS
VAV box controller (see Note 2 below)	Div 23	Div 23/BAS	BAS	Div 26
BMS conduits and raceway	BAS	BAS	BAS	BAS
Automatic dampers (non-factory)	BAS	Div 23	BAS	NA
Automatic valves	BAS	Div 23	BAS	NA
VAV boxes	Div 23	Div 23	BAS	NA
Pipe insertion devices and taps, including thermowells, flow and pressure stations.	BAS	Div 23	BAS	BAS
Air Flow devices, pressure sensors, and temperature sensors.	BAS	Div 23	BAS	BAS
BMS current switches	BAS	BAS	BAS	NA
BMS control relays	BAS	BAS	BAS	NA
All BMS nodes, equipment, housings, enclosures and panels (See Note 1)	BAS	BAS	BAS	BAS
Smoke detectors - duct mounted (see Note 3 below)	Div 28	Div 23	BAS/Div 26	Div 28
Firestats	BAS	BAS	BAS	Div 26
Fire/smoke dampers (see Note 4 below)	Div 23	Div 23	BAS	Div 26
Fire dampers	Div 23	Div 23	NA	NA
Fire alarm shutdown relay interlock wiring	Div 26	Div 26	Div 26	Div 26
Fire alarm smoke control relay interlock wiring	Div 26	Div 26	BAS	Div 26
Thermal Energy Meters (See Note 1)	Div 23/BAS	Div23/BAS	BAS	Div26/BAS
Dartmouth Water Meters (i.e. for Domestic Water)	Div 22	Div 22	BAS	BAS
Variable Frequency Drives (VFD)	Div 23	Div 23	BAS	Div 26

NOTES:

1. BMS low voltage and communications wiring: BMS Ethernet communications cable and IP infrastructure furnish by Div 25 and install by BMS Contractor or Division 26 Electrical Contractor as per options in paragraph above and as approved by Dartmouth College Network Services.

2. VAV box controller factory installation would normally be by Division 23 Mechanical who furnishes the VAV boxes; could be by BMS for field installation of special controllers.

3. Smoke detector also wired to shut down AHU/HVAC by Division 26.

4. Fire/Smoke Dampers: BMS Contractor to provide and ensure OPEN/CLOSE control and monitoring of fire/smoke dampers as coordinated between BMS HVAC systems sequences, controls and overrides, and the Fire Alarm system control status priorities and overrides.

END OF Appendix A

Appendix B: Dartmouth College Controls Vendor Standards for Building Controls Project Documentation and Software Control

Dartmouth College Controls Vendor Standards for Building Controls

Project Documentation and Software Control

The following are a list of standards for project implementation and software control for the Dartmouth College Controls Vendor Standards for Building Controls Project Documentation and Software Control. The purpose of these standards is to ensure that vendors coordinate with the College and provide complete as-builts and proper documentation of issues or software changes implemented.

1. Prior to any project implementation on an existing controls system, selected controls vendor shall perform a "system health assessment" to ensure that the existing system architecture and controllers are capable of supporting the proposed new logic without exceeding the manufacturers recommended configuration guidelines for acceptable amounts of points/devices/memory/CPU usage/etc. on that system. Furthermore, the vendor shall identify if there will be room for continued expansion within the system following implementation. If there are potential limitation issues identified, current system configuration/controllers exceed recommended guidelines, or new hardware or software will be needed, vendor shall make that known in writing to Dartmouth College Project Manager prior to starting any implementation. Conversely, if vendor does not anticipate an issue, that shall be communicated in writing as well.

2. Dartmouth College Building Automation Shop shall make the most current control software for existing systems available to the vendors in order to help them provide an accurate system health assessment.

3. All proposed graphics for a project shall be included as part of the initial project submittals. Failure to include graphics shall be cause for immediate rejection of submittals.

4. All device/controller/point names shall follow the standard "Dartmouth College Control System Naming Conventions" (see attached) unless otherwise requested by Dartmouth College.

5. Vendor shall provide to Dartmouth College Building Automation Shop a digital copy of all software that is currently configured in the system no later than the end of every work week with the understanding that it is to be used in case of emergency and not to be considered a final product.

6. All graphics that are related to equipment that is being worked on shall be in complete and working order before the end of that day so that after hours technicians may have a graphical view of the work that has been accomplished.

7. Vendors should label all thermostats to identify what controller they are connected to.

8. Vendors shall contact the Building Automation Shop on any day that they will be performing demolition or construction work on an existing control system. Also, the vendor shall inform the Project Manager and Building Automation Shop at the end of the work day the status of the controls system and confirm that there are no performance issues on existing systems prior to leaving the site.

9. Upon final completion and acceptance of a project, vendor shall provide a complete digital copy of all software from the project on the day of acceptance. This to include all end devices, building level controllers, graphics, etc. Vendor shall also provide complete construction as-builts and copies of control sequences in both digital and hard copy to appropriate Dartmouth College Shops (Building Automation and/or Electrical), and to Dartmouth Engineering. (As-builts to include electrician's communication bus routing diagram). Note that if project is a partial renovation to existing controls, as- builts shall be an update of original control system as-built digital and hard copy documents.

10. Vendors shall be given access to the control system (not including servers) in order to perform work but access shall be limited to 7:30am-4pm, Mon-Fri, unless an exception is required due to the project schedule.

DAY to DAY work:

11. Vendors that perform service work that is not considered a project may be given a copy of the software that they need in order to perform work that day, and that day only, with the expectation that they will return by disk or e-mail, a digital copy of that project if any changes were made, along with written documentation of changes made. Dartmouth College will then store the changed copy in a separate "working projects" folder until the changes made have been proven to provide the results requested. At that time, the file will be moved to Dartmouth College's secure project folder until a copy is requested again.

12. It is expected that the vendor may keep a copy of work performed in their company archives for reference but will delete said copy from their programming devices upon leaving the premises. Vendor shall request a new copy of software every day that they perform work in order to ensure that they do not use an out of date copy of software.

Dartmouth College Control System Naming Conventions

Note: Building Names/ Room Numbers to be coordinated with Dartmouth <u>Space System</u>

For Controllers:
Building.Floor.UnitName(with location served if a corridor/restroom/mech room).

IE: Wilder.Floor1.FCU1-Men's Room, Wilder.Floor1.AHU1 – Auditorium, or
Wilder.Floor3.VAV2

For controller descriptions, please note location served in description if a numbered controller and duplicate in alarm message text.
IE: Name - Wilder.Floor2.VAV3   Description – Serves Rm 201-202-203. Alarm Message Text - Serves Rm 201-202-203.

For Points:

Building.Floor.UnitName.PointName

IE: Wilder.Floor2.VAV4.Room202 RM Temperature or Wilder.Penthouse.AHU3.DA Temperature
In the point description, please use point name, location served and basic description of point.

IE: Description would be …. Wilder.Floor3.FCU12.SF-S - Rm201 Supply Fan Status Point
alarm message texts should give description of alarm such as shown below.

Note: Equipment assigned names should not duplicate names of other equipment in the building, eg.
two AHU-1's.

Additional Point Naming examples are given below.
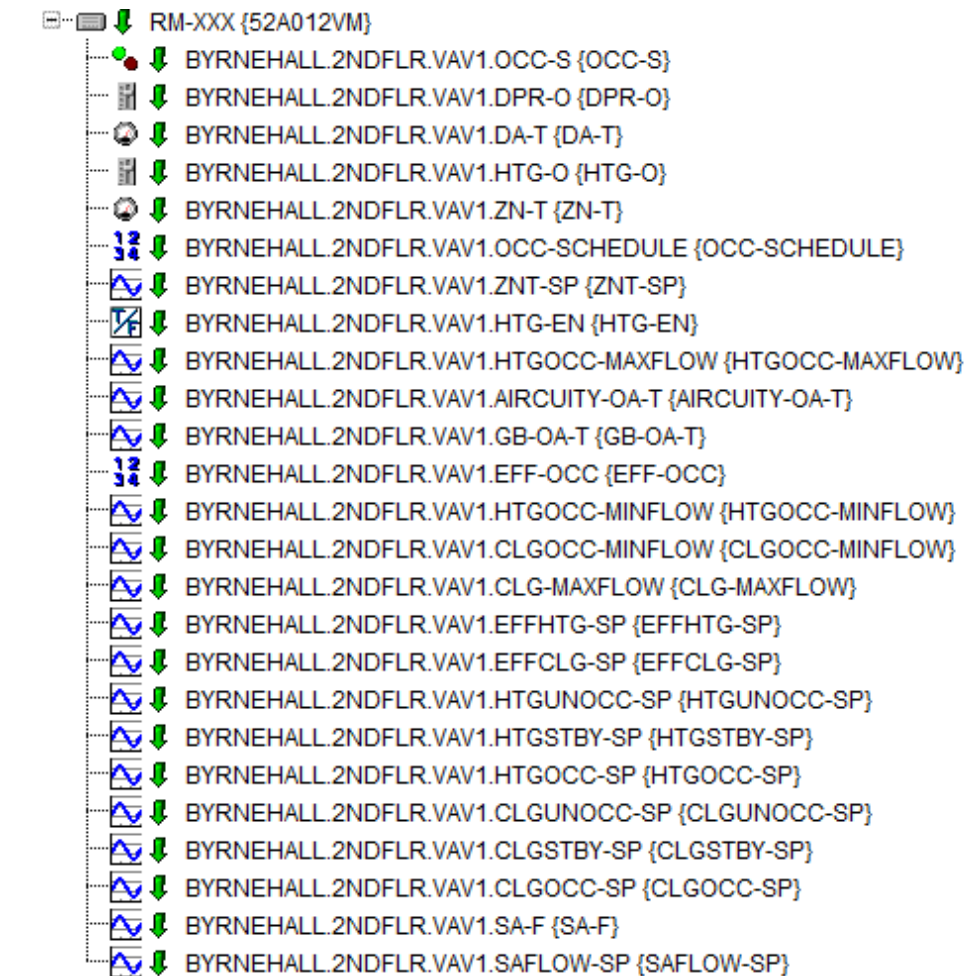
END OF Appendix B

Appendix C: Operational Technology Cybersecurity Policy

Executive Summary

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 guideline are intended to minimize these risks while preparing the organization to manage risk on an ongoing basis including recovering from a disastrous incident. These policies and procedures represent the minimum effort required to secure the technologies for this project and are intended to be utilized as a starting point for further development between the Owner and the BAS Contractor.

Revision History

General

ROLES AND RESPONSIBILITIES
OWNER and CONTRACTORS

General Responsibilities – Owner and Contractors

•May only access information needed to perform legitimate duties as an Owner employee or contractor and only when authorized by the appropriate information owner or designees.

•Are expected to ascertain and understand the sensitivity level of information to which he/she has access - through training, other resources, or by consultation with his/her supervisor or the information owner.

•May not in any way divulge, copy, release, sell, loan, alter, or destroy any information except as authorized by the information owner and within the scope of his/her professional activities.

•Shall understand and comply with Owner's requirements related to System and Information Integrity.

•Shall adhere to Owner's requirements for protecting any computer used to conduct Owner business, regardless of the sensitivity level of the information held on that system.

•Shall protect the confidentiality, integrity, and availability of Owner and client information - as appropriate for the information's sensitivity level - wherever the information is located (e.g., held on physical documents, stored on computer media, communicated over voice or data networks, exchanged in conversation).

•Shall handle information deemed confidential or highly confidential under this policy in accordance with Owner's requirements for protecting confidential and highly confidential information.

•Shall safeguard any physical key, ID card, or computer/network/system account that allows access to Owner information. This includes creating computer passwords that are compliant with the standards set forth in applicable Owner password policies and procedures.

•Shall destroy or render unusable any confidential or highly confidential information contained in any physical document (e.g., memos, reports) or any electronic, magnetic, or optical storage medium (e.g., USB key, CD, hard disk) before it is discarded in a method that is in compliance with applicable Owner media sanitization policies and procedures.

•Shall report any activities that he/she suspects may compromise sensitive information to his/her supervisor or to the Owner.

•Shall report any incidents as defined in Owner's Information Security Incident Reporting procedures to initiate an incident investigation.

•Shall meet obligations to protect sensitive information even after Owner employment or engagement ends.

•Shall contact the Owner and the Contracts Department before complying with any court orders, subpoenas, or other compulsory requests from Federal, state, or law enforcement agencies for disclosure of confidential information.

•If performing work in an office that handles information subject to specific security regulations, Shall comply with additional training and documentation requirements (e.g., acknowledge annually that he/she has read, understands, and agrees to comply with the terms of this policy).

Should any conflicting information arise, adhere to Dartmouth Information Security Policy
https://policies.dartmouth.edu/policy/dartmouth-information-security-policy

Owner Role

The Owner should familiarize themselves with their responsibilities as it pertains to the policies and procedures outlined in this document.

The Owner should understand that their input will be necessary to complete this implementation in a secure and sustainable manner.

The Owner should understand that the policies and procedures in this document are intended to be the basis for an Operational Technology Cybersecurity Policy, to which will be the standard for implementation of the Division 25 guideline and it is recommended that the Owner augment the policies, should they be properly equipped with knowledgeable personnel.

BAS – Building Automation System Contractor Role

The BAS – Building Automation System Contractor should familiarize themselves with their responsibilities as it pertains to the policies and procedures outlined in this document.

The BAS – Building Automation System Contractor shall adhere to and augment this set of policies by leveraging their qualifications, experience, and industry best practices.

BAS Contractor Responsibilities

The BAS – Building Automation System Contractor is responsible for ensuring that all systems comply with the cybersecurity requirements defined within this guideline.

The BAS – Building Automation System Contractor will be responsible for documenting all devices and related software integrations added outside of the original project design specifications.

Prior to project turnover, commission the Integration Platform and all connected subsystems provided by the Integrated System Contractors based on the defined cybersecurity policies and procedures.

The BAS – Building Automation System Contractor will provide the Owner with a written commissioning report summarizing the compliance findings across all systems.

OWNER POLICY – CYBERSECURITY for DIVISION 25 GUIDELINES

The following policies are to be finalized and updated with the Owner prior to project implementation and again prior to completion in conjunction with the BAS – Building Automation System Contractor. In some cases, the policies apply to post-construction support during and after the warranty period.

End User Account Policy

Encryption Policy

Internet Connectivity Policy

Remote Communications Policy

System Backup Policy

Disaster Recovery Policy

Integrations Platform Host Management Policy

System Component Cybersecurity Configuration Policy

End User Account Policy

Account Creation

The Owner shall be able to manage and audit all accounts.

The Dartmouth College BAS Shop is the authorized entity to add user accounts to all systems related to the integration platform.

The BAS CONTRACTOR must adhere to the following guidelines:

Account Authorization

Authorization of Users

> The Dartmouth College BAS Shop will have the responsibility to manage all user account access.
>
> The Dartmouth College BAS Shop will create user accounts and associate levels of access.
>
> The Dartmouth College BAS Shop will record all user accounts and associated levels of access.

Creation

> The Dartmouth College BAS Shop will have the responsibility to create user accounts necessary for system access.
>
> The Dartmouth College BAS Shop will be responsible for assigning the appropriate level of access to the user account.

Removal

> The Dartmouth College BAS Shop will have the responsibility to remove user accounts.
>
> The Dartmouth College BAS Shop will remove accounts, either through suspension or deletion, within one business day for individuals who:
>
> > No longer employed and require access
> >
> > Had job responsibilities reassigned and no longer need access.

Audit

> The Dartmouth College Campus Services Technology Services (CSTS) will be responsible for performing a User Account Audit no less than every 3 months to ensure that only authorized user accounts remain and that the associated privileges are consistent to their role.
>
> The Dartmouth College Campus Services Technology Services (CSTS) will review the audit results with Dartmouth College BAS Shop.
>
> The Dartmouth College Campus Services Technology Services (CSTS) will securely archive the audit results for a period of 2 years to ensure historical availability.

Administrative Users

> The Dartmouth College BAS Shop will ensure that a minimum of 2 Full Administrators and a maximum of 4 with at least one administrator being an Owner employee.

> System administration privileges should be granted to individual accounts whose role requires this privilege in order to fully configure and program the system, including creating new accounts.

Guest Users

> No Guest user accounts should exist on any system.

> The Dartmouth College Campus Services Technology Services (CSTS) will be responsible for disabling or removing Guest user accounts from all systems prior to device installation and after an audit has been performed.

Generic User Accounts

> No Generic user account will be used on any system.

Manufacturer Default User Accounts

> No Default User Accounts will be used on any system.

> All Default user accounts must be deleted or if unable to be deleted, the password must be changed per the Password section of the End User Account Policy and then recorded prior to installation.

Non-User Service Accounts

> These may be accounts that allow access between devices or between software platforms and device.

> Service accounts or non-user accounts (a.k.a. Machine Accounts) are the responsibility of the Dartmouth College BAS Shop.

> API communications are the preferred method of integration.

> The Dartmouth College BAS Shop must configure and manage these accounts according to the Owner's End User Account Policy.

Account Authentication

Passwords

> Passphrases shall be utilized in lieu of passwords where permissible by the system being secured.

> The Dartmouth College Campus Services Technology Services (CSTS) is responsible for managing and enforcing the Passphrase Policy for user accounts associated with applications and Operating Systems.

> Each user account is to have a unique Passphrase

> No shared user account Passphrases

> Passphrases for user accounts must adhere to Dartmouth Information Security Policy https://policies.dartmouth.edu/policy/dartmouth-information-security-policy

>> Contain a combination of upper case, lower case, numeric, and special characters.

> Passphrases must not be reused.

Passphrases must be changed upon initial end user log on.

Passphrases must be changed at a 90 maximum.

No hard-coded, factory default, or otherwise well-known passwords, passphrases, PIN numbers, or other credentials may remain configured in any system following Commissioning.

Account Accounting

Logging

The Dartmouth College Campus Services Technology Services (CSTS) is responsible for enabling logging for all user account activity on all applications and Operating Systems that comprise the integration solution.

These logs should be remotely collected by a host that should be managed by both the Owner's Backup Policy and Owner's Disaster Recovery Policy.

These logs should be reviewed monthly for suspicious administrative activities.

These logs should be retained for a minimum of 2 years.

Encryption Policy

All communications that transmit system data shall be encrypted. Examples include all GUI sessions, CLI sessions, endpoint compute devices, APIs, device to device (if feasible), etc.

Encryption standards and methodologies established should align with (b) Cybersecurity Practice Guide Special Publication 1800-16 Securing Web Transactions: TLS Server Certificate Management.

The recommended encryption is TLS 1.2, TLS 1.3.

Obsolete encryption protocols such as SSL 2.0, SSL 3.0, TLS 1.0, and TLS 1.1 shall not be implemented.

Ownership of all certificates comprising the integration solution must be defined.

All device and application certificate expiry dates must be inventoried and a method for renewal must be established.

All device and application certificates must be valid.

Internet Connectivity Policy

Internet connectivity shall be managed by the Owner.

System access to the Internet must be requested of the Owner and will be granted at the Owner's discretion.

Requests for Internet Connectivity must include outbound transmission ports and destination IP Addresses.

Remote Communications Policy

No components of the integration solution will be public facing.

Connections from outside the local area network are to be made through a VPN or other remote access

solution (i.e. remote desktop products to a secured, internal workstation; TosiBox, Tempered Networks, etc.)

VPN policy management is by the Owner. Remote access to be coordinated with the Dartmouth College BAS Shop.

Installation and/or use of remote access software such as TeamViewer, Bomgar, VNC, GoToMyPC, or similar is forbidden without formal approval by and coordination with Dartmouth IT Security.

System Backup Policy

All service host platforms (i.e servers that host application, database, domain, syslog, etc.) must have a system image backup performed by an enterprise grade backup service and include daily incremental changes.

Backups are to be stored in a secure location with redundancy.

Backups are to be tested for integrity and restoration capability verified periodically

Systems capable of backing up downstream device configurations are to be configured to do so.

If no system exists to backup downstream device configurations, a manual backup should be made every two months and prior to any device programming change, a backup copy of the current configuration must be preserved.

Backups should be retained for a minimum of 6 months.

Cloud-based hosted solutions are required to provide an outline of data retention and solution backups.

Disaster Recovery Policy

The Owner will work with the BAS CONTRACTOR to establish a Disaster Recovery Plan.

The following topics to be included at a minimum are:

System and system component outage impact

Ownership of each system and each response

Backup and restoration procedures

Manual operations

Communication plan

Failure analysis

Annual testing procedure to include fail-over testing against recorded commissioning procedures.

PRODUCT HARDWARE

Integrations Platform Host Management Policy

The BAS CONTRACTOR and Owner will determine at the onset of the project whether management of the Integration Platform Host (day-to-day, backups, disaster recovery, etc.) is to be the responsibility of the Owner or the BAS CONTRACTOR under a separate service agreement. The BAS CONTRACTOR will

follow these guidelines for implementation.

The Host may either be a physical server located onsite or a cloud hosted platform. The following policies will be applied per type:

Local Server

Physical Environment:

The server will be located in a secure environment.

Only intended administrators of the server are to physically access the system.

The server should reside in a lockable enclosure.

Keyboard, mouse, and monitor should not be attached when not in use.

Unauthorized individuals should not be able to plug in any USB device.

The environment should be secured via Key Access (minimum) or Electronic Credentialed Access Control System (recommended).

A recording surveillance camera(s) should be installed to monitor the enclosure and ingress/egress point(s).

Programming:

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.

The operating system (OS) software must be running a fully supported version with all security patches installed with a documented methodology to continue patching as necessary updates are released.

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

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

*Additional Host Server Platforms are recommended for other service functionalities such as Syslog Archive, Domain Services, RADIUS, DHCP, etc.

Cloud Hosted

A Cloud Hosted Integration Platform shall comply with the following policies and procedures:

End User Account Policy

End User Authentication Policy

End User Authorization Policy

End User Accounting Policy

Encryption Policy

PRODUCT SOFTWARE

Product software licensing managed by Dartmouth College BAS Shop in coordination with the BAS Contractor(s).

System Device Cybersecurity Configuration Policy

Purpose:

This policy defines the standards for configuring system hardware devices for standalone installation or integration.

Application of Policy:

This applies to any system that has a user interface (CLI or GUI or Discovery Tool) for modifying the software on the device.

Application Software

The device shall be currently fully supported by the manufacturer and installed to the latest software release level.

Encryption

At a minimum, all device communications must be encrypted using the strongest encryption available on the device. Recommendations include TLS 1.2 and TLS 1.3 (preferred). Obsolete encryption protocols such as SSL 2.0, SSL 3.0, TLS 1.0, and TLS 1.1 must not be implemented.

Cyber Security Dashboard (GUI)

  i.   The Cyber Security Dashboard shall provide a centralized view of potential cybersecurity related issues or system issues, grouped into critical issues, potential risks, and informational items.

  i.   The Cyber Security Dashboard shall identify user account information, including:

       a.   Total number of users

       b.   Dormant users

       c.   Active users

       d.   Locked users

       e.   Temporary users

       f.   Disabled users

       g.   Users with Administrator role

       h.   Policy related information

     ii.   The Cyber Security Dashboard shall indicate out-of-date software and Firmware.

     iii.   The Cyber Security Dashboard shall identify when security certificates are set to expire.

     iv.   The Cyber Security Dashboard shall provide insight into user activity such as number of successful logins, unsuccessful logins, and locked out accounts.

Securing System Access

If the system provides multiple methods for administrative interaction, it must be configured according to the table below.

GUI - HTTP	GUI - HTTPS	CLI – Telnet	CLI – SSH	CLI – Console
Disable	Enable	Disable	Enable	Via Auto-Logoff

User Accounts

All Administrative User Accounts should be created according to the Owner's End User Account Policy.

Guest Accounts

Must be disabled or removed if option is available per the Owner's End User Account Policy.

Default Accounts

Must be removed or replaced with an Authorized User Account(s) during installation per the Owner's End User Account Policy.

Auto-Lockout

If an auto-lockout feature is available, it must be enabled and configured for no more than 5 login attempts.

Auto-Logoff

If an auto-logoff or "timeout" feature is available, it must be enabled and configured to disconnect an Authorized User Account after 15 minutes of inactivity. This applies to all methods of administrative access.

Activity Logging (SYSLOG)

If the system has the ability to log events, it must be enabled and configured to record all activity (user, system) for a minimum of 1 week and/or be configured to send its log(s) to a remote secure archive.

Multiple Communication Interfaces

If the system has multiple communication interfaces, all interfaces not in use must be disabled. If unable to disable, then the methods should be hardened against discovery and direct connectivity though whatever means is available on the device to do so. I

IPMI management Interfaces

Disable IPMI management when not in use

IF system has IPMI Network interfaces, these must only be connected to dedicated management networks.

EXAMPLE: A system component has the following communication interfaces:

       Ethernet port – Primary

       Ethernet Port – Secondary

       WiFi Radio

       Bluetooth or BLE Radio

       Console Port

Only the Primary Ethernet port will be used for communications. All other interfaces must be disabled via device programming. Should interface disablement not be an option, then steps must be taken to harden via changing pass phrases, etc.

<p style="text-align:center">END OF Appendix C</p>

Appendix D: Integration Checklist

Integration Checklist

For Owner: [   ]

Project Data

Project Name	[ ]	Integrator/SI/MSI	[ ]
Site Location	[ ]	Contact Name	[ ]
Building Name	[ ]	Contact Phone	[ ]
		Email	[ ]

Device Data   *Select From Drop-Down*   **Device Communication**

Type of Device   [Choose an item.]   Device IP (If Static)   [   ]

Control/System   *Select From Drop-Down*

Type of Control   [Choose an item.]   Device MAC Address   [   ]

Protocol   *Select From Drop-Down*

Protocol Used   [Choose an item.]

Demark Location   [   ]   **Device Location**   [   ]

IP Scheme required?   Y/N

No. of IP Addresses?   [   ]

Integration Point Mapping Supplied?   Y/N

Device Cut Sheets with Model Supplied?   Y/N

END OF Appendix D