WASHBURN UNIVERSITY

WORKSHEET A - RFI 25026 Electronic Lock Access Control

VENDOR NAME:

CATEGORY	WASHBURN UNIVERSITY REQUIREMENTS	**Supplier Response:** Please detail how Supplier's proposed products are currently able to provide each of the items listed in Column B.
Architecture	Proposed solution must interface to 'Mercury Security' controller panels	
Architecture	All hardware and software must support Open Supervised Device Protocol (OSDP)	
Architecture	Product works with Assa Abloy (HID) readers	
Architecture	Product works with Assa Abloy (HID and Sargent) lock hardware	
Architecture	Describe power draw per device for all proposed equipment that uses PoE (Power over Ethernet)	
Architecture	Describe how readers are programmed and updated. (Centrally managed?)	
Architecture	High availability and redundancy-database, failover.	
Architecture	Cloud capabilities for remote management and access.	
Architecture	Describe the options for hosting the system (e.g. cloud, on-premise, hybrid)	
Architecture	Open architecture design to facilitate integration and future expansion with third-party systems, such as, Banner database, Supplier should list current integrations with third party systems.	

Architecture	Describe in detail how system currently integrates with Power Over Ethernet (POE)/Aperio/Wi-Fi locksets	
Architecture	Describe how regular software updates and security updates are applied.	
Camera - Functionality	Software integrates with or incorporates CCTV cameras and surveillence systems, including Pelco, Avigilon, and Axis cameras	
Camera - Functionality	Interactive digital Map of camera and electric lock locations to facilitate system operation	
Camera - Functionality	License Plate Reading (LPR)	
Camera - Functionality	Object of interest searching capabilities	
Camera - Functionality	Tracking indivduals across multiple cameras live/review	
Camera - Functionality	Ability to give certain users/roles permissions through the software to: reboot camera, create PTZ patterns, configure motion detection, and other analytic features; without giving users direct login access to camera	
Camera - Functionality	Automated reporting for various information. - offline cameras, recording gaps and esc	
Camera - Functionality	Intuitive video exporting system that's reviewable by 3rd parties	
Camera - Functionality	Ability to update firmware and other settings on cameras in mass	
Camera - Service	24/7 on call support team. For both troubleshooting of system and assistance in implementation of features	
Camera - Service	Training program and materials for end users.	
Camera - Technical	Provide 500 cameras 30-days of recording. At current setup estimated to be 200TB of storage	
Camera - Technical	Recording system built to handle at least 1Gb of throughput	
Camera - Technical	Video Management software - ONVIF Compliant	

Camera- Functionality	Basic analytical capabilities - Loitering, motion detection, tampering detection, and esc	
Functionality	Robust lockdown features allowing lockdown from single doors to whole campus at once	
Functionality	Real-time central station monitoring and alerts for security incidents	
Functionality	Monitoring supports map displays with drilldown	
Functionality	Supports multiple monitoring and control stations	
Functionality	Describe what functionality remains available in the event of a total data network outage	
Functionality	Supports HID Seos cards	
Functionality	Supports RFID and NFC communication	
Functionality	Supports integration with Apple Wallet and Google Wallet	
Functionality	Access may be granted to and cards may be printed for persons not in the Active Directory; guest passes	
Functionality	Support for unlimited time intervals for door schedules, for a complex university setting	
Functionality	Allows for a variety of authentication options, including biometric, RFID cards and devices, NFC devices, and PIN codes. These should be customizable based on access requirements.	
Functionality	Full Access for multiple concurrent Users to Administrate the Platform	
Functionality	Washburn has identified approximately 50 users. Please provide cost to add users beyond initial 50 with price locked in for the duration of the contract period.	
Functionality	Current ability of Supplier to provide support for mobile credentials to enable secure access using smartphones.	
Functionality	Centralized management and configuration for administration users, while utilizing a distributed management system to partition to user groups.	

Functionality	Real-time monitoring and alerts in a central station environment (intrusion detection, door propped)	
Functionality	Must currently have ability to place intrusion systems on test to minimize disruptions to dispatch	
Functionality	Visitor management functionality	
Functionality	Mobile/Web application for users and administrators	
Functionality		
Functionality	Intrusion detection and panice systems to trigger alarms and notifications for a Digital Monitoring Products intrusion system (DMP)	
Functionality	Real-time Central Station monitoring and alerts for security incidents. With graphic maps and video capabilities.	
Functionality	Intuitive and user-friendly administrative interface	
Functionality	Access control software needs to be compatible with Signo Readers, Sargeant IN120 and IN220, and Aperio Locks.	
Functionality	The solution should be highly scalable to accommodate the growth of the campuses. It should easily adapt to the addition of new buildings, facilities, and users without significant disruptions or architectural changes.	

Functionality	Multi-factor authentication options (including, but not limited to: SEOS, HID Prox, HID mobile credential)	
Functionality	The solution must support a variety of secure user authentication methods, including biometric authentication, RFID cards, PIN codes, and mobile credentials. These authentication methods should be customizable based on access requirements.	
Identity Access	Identity Management Systems for synchronization of user data and permissions Single sign-on (SSO) is a session and user authentication service that permits a user to use one set of login credentials -- for example, a name and password -- to access multiple applications.	
Identity Access	Authentication is a process by which users, processes, or services provide proof of their identity. User authentication often relies on a username and password but may also require a second authentication factor (e.g., DUO) where greater assurance of identity is required. Requirement: The application will integrate with existing Washburn University authentication systems and protocols to authenticate users, processes, and services.	
Identity Access	The application must accommodate a username in the format of an email address.	
Identity Access	The application must support CAS or SAML2 protocols using the University's supported identity providers (Ellucian Ethos Identity Services and Azure) backed by Active Directory.	
Identity Access	In the case of SAML2, the vendor must be able to provide a metadata.xml file or URL to the service provider's metadata. Any attributes required for user identification or authorization must exist in Washburn's Active Directory.	

Identity Access	Preferred MFA (Multi Factor Authentication) Integration with DUO (Identity Management and Single Sign-On; SAML).	
Identity Access	Authorization includes processes that ultimately control what a user or process is allowed to do in an application. These processes may include organizing users into groups, assigning users or groups to roles, and managing the permissions for each role on application resources. Requirement: The application will integrate with existing University services to manage groups, roles, and permissions. The application must have a Role Based Access Control (RBAC) model that is sufficiently flexible to meet the University's business needs.	
Identity Access	The application's Role Based Access Control model can be extended to accommodate the University's custom roles if necessary (affiliate, for example).	
Identity Access	The application can map groups or individuals into roles.	
Identity Access	The application can accommodate multiple roles per user without requiring multiple accounts (employee that is a student, for example).	
Identity Access	If the application requires creation of local accounts in order to facilitate authentication or authorization, this must be approved by the Washburn University CIO.	
Identity Access	Describe in detail what Multi Factor Authentication (MFA) solutions the Supplier's proposed solution currently supports to access the system. (for example: Active Directory, Duo, etc.)	
Installation	Vendor will provide on-site usage and troubleshooting training to administrators, operators, and technicians	

Installation	Vendor will install and configure software to replicate current setup including device groups, user groups, and access levels, for components that the software will manage.	
Installation	Vendor will install new hardware and verify correct operation	
Integrations	API integration capabilities (Banner/AMT Database)	
Integrations	Describe APIs for input and output to third-party systems	
Integrations	Are you an Ellucian partner? If so, what level?	
Integrations	Please describe in significant detail how integration with Banner works. (flat files, Ethos, views, direct database access, API, other)?	
Integrations	Please provide a list of all data elements that you will read from the Banner database and why they are necessary to its functionality.	
Integrations	Please provide a list of all data elements you will push back into the Banner database.	
Integrations	Is any additional hardware or software required to support the integration? Describe.	
Integrations	Provide a detailed diagram depicting the integration.	
Integrations	Will your software need to access other data sources? Describe.	
Integrations	How many other Banner customers are you currently integrated with?	
Integrations	Describe options for timeliness of data integration (daily, hourly, real-time?)	
Integrations	Optional Integration Items depending on the application:Washburn has implemented Ellucian Ethos. If your product requires Ethos for data exchange, please describe in detail the fields exchanged.	

Integrations	Describe the Supplier's proposed systems current ability to expand to future API's for unknown future integrations.	
Reporting	User defined specific events.	
Reporting	Describe in detail the data retention abilities of the proposed solution and the extent to which this is configurable. Detail any external storage options available.	
Reporting	Customizable reporting and analytics tools for access logs and occupancy trends.	
Reporting	User defined scheduling of unlimited user defined reports with output to email or file.	
Reporting	Master Events History – Shows date, time, door hardware location, WIN, Name of person Washburn Police & Residential Living will request these reports. On occasion other departments will request for various reasons.	
Reporting	Master Cards Listed by Cardholder Name – shows WIN, name, access and an access level, expiration date if manually added, interface/import access (this is used for class rosters, Residential Living for those living on campus, Law School faculty/staff/students) if someone leaves the university, drops a class, moves out of their residence hall access is removed automatically if taken out of the Banner system which feeds the interface/import.	

Reporting	Various Door Access Schedules – We have many schedules for exterior, interior, after hours, holidays, etc. These schedules constantly change and are flexible. Process – Set up a schedule which consists of days, times, holiday schedule if appropriate. Door Group – Door(s)/Readers assigned to the door group. Access Level – Add Door Group/Schedule Scheduled Commands – Assign a scheduled command (open) to a device (door/reader)	
Reporting	Adding/removing access for individuals – Manual access add the access level name and effective dates. To remove access, delete the access in the software. Interface/Import access is added by various departments by going into banner and adding a CRN and expiration date, Residential Living uses StarRez/Banner to update or remove residence access. Interface/Import access is removed when expiration date is applied or individual is removed from Banner.	
Security	Describe how proposed solution meets Washburn's Security requirements	
Security	Vendor possesses SOC 2 Type II certification for data security and privacy compliance	
Security	Must be natively capable of AES-128-bit Open Supervised Device Protocol (OSDP) encryption from reader to panel for enhanced security.	
Security	Certification with ISO 27001 (Information Security Management System) and ISO 27017 (Cloud Security) standards.	
Security	Certification with UL 294 (Standard for Access Control System Units) standard.	
Security	Ability for Full functionality in event of network outages	

Security	Describe in detail how Supplier's proposed solution currently supports Role Based Access Control (RBAC). Describe the granularity Supplier's proposed system currently allows for RBAC. Describe the different permissions and user roles that are natively available to the proposed application.	
Security	Has a HECVAT been completed and submitted with your proposal	
Security	Describe how your proposed solution will store and transmit data in a secure fashion.	
Service	Vendor is certified by the manufacturer (and personnel are themselves certified, if applicable) to install and service the HW and SW proposed in the bid.	
Service	Vendor is certified as an Assa Abloy integrator (and personnel are themselves certified, if applicable)	
Service	Must provide a service-level agreement (SLA) that stipulates vendor will be able to perform on-site service within 24 hours of service call	
Service	Vendor must provide telephone support with response of 4 hours or less after reported issue.	
Session Management	Session Management provides capabilities to control properties of a user's session such as session length, forced reauthentication, and logout. The primary goal of “Session Management” requirements is to ensure that data security controls on user application sessions can be configured to meet current and anticipated business needs. (Role-based access control). Requirement: The application will allow configuration of user session controls that meet University security and privacy needs.	
Session Management	The application has a configurable user session inactivity timeout.	
Session Management	The application supports user-initiated logout.	

Technical	If proposed solution is a hosted cloud web-based solution, with sufficient memory/data to ensure top speed for all system processes and must provide adequate support for its system and users including but not limited to (1) a dedicated team who is familiar with or will be fully familiar with the University's setup, exceptions and processes, (2) direct access to the team, via phone and email during regular business hours.	
Technical	All University data must be stored and backed-up within the continental United States of America. In no event shall the University's data be accessed, transferred, or stored outside of the USA. Please describe and provide diagrams of exactly how storage and data are protected from external penetration of the information in the proposal.	
Technical	The proposed software solution must be off-the-shelf (pre-programmed); generally available (i.e., not in beta or test) and currently in production and in use in or accessed by a client environment as proposed. Prototypes or items in test production and not formally announced for market availability shall not be accepted. All equipment, products, and supplies offered in the proposal must be new, of current production, and available for marketing by the manufacturer.	
Technical	The configuration selected must be flexible, and provide the ability to scale with the University.	
Technical	The solution should be intuitive and easy to use for all users.	

Technical	The solution must be compatible with current common browsers and maintain compatibility to newer versions of common browsers such as FireFox, Edge, Chrome, and Safari.	
Technical	The solution should have the ability for persistent audit and authentication logging.	
Technical	The solution should allow for direct database access to raw data to support Washburn's automated data analytics initiatives.	

Technical	The University is subject to the European Union's General Data Privacy Regulation [Regulation (EU) 2016/679] (the "GDPR") when the University is a "controller" or "processor" of "personal data" from an individual "data subject" located in the European Union, as those terms are defined in the GDPR. The Contractor acknowledges and agrees that it is acting as a "processor" of "personal data" for the University under the resulting Contract Agreement and that all applicable requirements of the GDPR are incorporated by reference as material terms of the resulting Contract Agreement. The Contractor represents and warrants that (1) it is aware of and understands its compliance obligations as a "processor" under GDPR; (2) it has adopted a GDPR compliance policy/program; (3) it will process "personal data" only in accordance with the University's instructions; and (4) with regard to its obligations under any resulting Contract Agreement, it shall comply with all applicable requirements of the GDPR to the same extent as required for the University. Additionally, the Contractor shall indemnify and hold the University, its trustees, officers, and employees harmless from and against any claims, demands, suits, damages, penalties, fines, or costs arising from any violation of GDPR by the Contractor.	
Technical	The proposed solution should be capable of interfacing with the following third-party software systems: (1) Ellucian Banner; (2) Ellucian's Self Service; (3) Intergration with Ellucian Partner Imaging.	
Technical	Describe how the proposed product is compliant with FERPA.	