YOUNGSTOWN STATE UNIVERSITY

BOARD OF TRUSTEES
FINANCE AND FACILITIES COMMITTEE
Michael A. Peterson, Chair
Allen L. Ryan, Jr., Vice Chair
All Trustees are Members

Wednesday, March 1, 2023
11:30 a.m. or immediately following previous meeting

Board Room
Tod Hall

AGENDA

A. **Disposition of Minutes for Meeting**

B. **Old Business**

C. **Committee Items**

1. **Finance and Facilities Consent Item***

C.1.a. = Tab 1

a. **Resolution to Modify Purchasing Policy, 3356-3-01**
Neal McNally, Vice President for Finance and Business Operations, will report.

2. **Finance and Facilities Action Items**

C.2.a. = Tab 2

a. **Resolution to Modify Acceptable Use of University Technology Resources Policy, 3356-4-09**
Jim Yukech, Associate Vice President and Chief Information Officer, will report.

C.2.b. = Tab 3

b. **Resolution to Approve an Increase to the International Application Fee**
Neal McNally, Vice President for Finance and Business Operations, will report.

3. **Finance and Facilities Discussion Items**

C.3.a. = Tab 4

a. **Quarterly Update on the FY 2023 Operating Budget**
Neal McNally, Vice President for Finance and Business Operations, will report.

C.3.b. = Tab 5

b. **FY 2024 Budget Planning**
Neal McNally, Vice President for Finance and Business Operations, will report.

*Items listed under the Consent Agenda require Board approval; however they may be presented without discussion as these items include only non-substantive changes.

C.3.c. = Tab 6

c. Planning and Construction Projects Update
John Hyden, Associate Vice President for Facilities and Support Services, and Rich White, Director of Planning and Construction, will report.

C.3.d. = Tab 7

d. IT Update
Jim Yukech, Associate Vice President and Chief Information Officer, will report.

e. Report of Audit Subcommittee
A verbal report of the Audit Subcommittee will be presented.
Michael A. Peterson will report.

D. New Business

E. Adjournment

YOUNGSTOWN STATE UNIVERSITY

RESOLUTION TO MODIFY
PURCHASING POLICY, 3356-3-01

WHEREAS, University Policies are being reviewed and reconceptualized on an ongoing basis; and

WHEREAS, this process can result in the modification of existing policies, the creation of new policies, or the deletion of policies no longer needed; and

WHEREAS, action is required by the Board of Trustees prior to replacing and/or implementing modified or newly created policies, or to rescind existing policies.

NOW, THEREFORE, BE IT RESOLVED, that the Board of Trustees of Youngstown State University does hereby approve the modification of the University Policy stated above and attached hereto.

Board of Trustees Meeting
March 2, 2023
YR 2023-

3356-3-01 Purchasing.

Responsible Division/Office:	Procurement Services
Responsible Officer:	VP for Finance and Business Operations
Revision History:	June 1998; June 2001; March 2007; May 2010; January 2012; December 2016; June 2017; June 2022; March 2023
Board Committee:	Finance and Facilities
Effective Date:	**March 2, 2023**
Next Review:	2028

(A) Policy statement. Employees who are delegated signature authority for university accounts are authorized to make purchasing decisions for their respective areas, following applicable university procedures. In all its business practices, the university will adhere fully to all applicable laws, regulations, and rules of the federal, state of Ohio, and local regulatory bodies. Those conducting business for the university will seek to obtain the best value when making purchases, while protecting the interests of Youngstown state university (university).

(B) Purpose. This policy helps ensure compliance with applicable federal and state purchasing regulations and provides a means for purchasing at a reasonable cost.

(C) Definitions.

(1) "Goods" are defined as, but not limited to, equipment, materials, other tangible assets, and insurance, but excluding real property or an interest in real property.

(2) "Services" are defined as any deliverable resulting from labor performed specifically for the university, whether from the application of physical or intellectual skills. Services include repair work, consulting, maintenance, data processing, and software design. Services do not include services furnished pursuant to employment agreements.

(3) "Professional design services" are defined as, but not limited to, services within the scope of practice of a state-registered architect,

registered engineer, registered surveyor, landscape architect and interior designer. See rule 3356-4-07 of the Administrative Code (university policy 3356-4-07, "Selection of design professionals for university capital projects").

(4) "Construction renovation" is defined in rule 3356-4-15 of the Administrative Code (university policy 3356-4-15, "University construction/renovation projects").

(D) Parameters.

(1) Accountability for vendor commitment and/or the actual purchase of goods or services rests with the financial manager. All construction/renovation projects must be coordinated through the university's facilities office.

(2) Procurement services has the primary responsibility to manage and monitor the purchasing process. Authority is delegated to the Maag library to purchase items to be added to its collection.

(3) As a commitment to diversity, equity and inclusion, the university provides opportunities for socially and economically disadvantaged businesses and participates in the state of Ohio's minority business enterprise (MBE) and encouraging diversity, growth and equity (EDGE) programs.

(4) To ensure the best value and compliance with applicable federal and/or state of Ohio regulations, the university requires competitive selection for certain dollar thresholds and participates in competitively awarded governmental and group purchasing agreements.

(E) Procedures.

(1) Requests for purchases are made by using a university-approved procurement card or the online procurement requisition system.

(2) An authorized electronic requisition/purchase order for goods or services must be processed through procurement services prior to vendor commitment and/or the actual purchase except for authorized procurement card purchases. Exceptions may be made in the case of an emergency, such as, but not limited to,

unexpected building repairs that could otherwise result in catastrophic structural failure.

(3) All purchases for goods and services for which there is an existing university contract or price agreement with one or more preferred vendors must be made from those vendors. This applies regardless of payment method (purchase order, p-card, etc.). Some existing university contracts and agreements can be found on punch out catalogs on the university's online procurement system. Instances where significant cost savings can be achieved by purchasing from a vendor not on an existing university contract or price agreement requires approval by the director of procurement services, or designee, prior to vendor commitment and/or actual purchase.

(4) If there is no existing university contract available, procurement services can assist in locating an approved competitively awarded governmental or group purchasing agreement, such as state term schedule, general services administration schedule, inter-university council purchasing group, or others.

(5) Competitive selection dollar thresholds.

(a) Goods or services when an individual transaction/project from a single supplier is fifty thousand dollars or more.

(b) Professional design services when an individual transaction is fifty thousand dollars or more.

(c) A construction/renovation project when the construction project cost is two hundred fifteen thousand dollars or more or the threshold established by rule 153:1-9-01 of the Administrative Code.

(6) For purchases below the competitive selection dollar thresholds, the director of procurement services, or designee, may require a minimum of three quotes or a competitive selection process when in the best interest of the university to do so or when regulations require.

(7) For purchases at or above the competitive selection dollar thresholds, appropriate forms of competitive selection include:

(a) An invitation to bid (ITB). A formal ITB is drafted and sent to prospective bidders and published in appropriate media when seeking to purchase goods.

(b) A request for proposal (RFP). RFPs are managed and distributed through the university's procurement services office. An RFP is drafted and sent to prospective bidders and published in appropriate media when seeking to purchase goods.

(c) A request for qualifications (RFQ). With the assistance of procurement services, an RFQ is sent to prospective bidders and may be published in appropriate media when seeking to purchase services. RFQs for professional design services are handled solely through the facilities office.

(d) Purchases under an approved competitively awarded governmental or group purchasing agreement, such as state term schedule, general services administration (GSA) schedule, inter-university council purchasing group, or others, some of which can be found on punch out catalogs on the university's online procurement system (eCUBE).

(8) Exceptions to competitive selection requirements.

(a) Maintenance contracts purchased from the manufacturer or authorized dealer/supplier of the specific equipment to be serviced.

(b) Software/hardware for system upgrades and ongoing maintenance and support on existing systems already in use.

(c) Special circumstances, including single source provider, emergency purchases, or economic efficacy. If the purchase is at or above the competitive selection dollar threshold and the nature of the purchase is such that competitive selection would be impractical, the department making the request for a purchase may submit a written request for a waiver of competitive selection. Such requests must include justification as to why a waiver is

warranted, be signed by the appropriate financial manager with signature authority, and be attached electronically to the requisition being submitted for the purchase.

If the director of procurement services, or designee, finds that sufficient justification has been presented, the waiver may be approved. If the director, or designee, feels that a bid waiver should be denied, it will be forwarded to the vice president for finance and business operations, or designee, for a final determination. If the request is denied, procurement services will initiate a competitive selection process at the request of the department end user.

(9) Bidding thresholds may be adjusted to comply with federal and/or state regulations.

(10) Contract compliance and administration processes will be conducted in accordance with rule 3356-3-04 of the Administrative Code (university policy 3356-3-04, "Contract compliance and administration").

(11) The university assumes no obligation for any purchases made outside of the purchasing procedures established herein. Staff who fail to follow approved processes may be subject to personal financial liability and appropriate disciplinary action.

(12) Purchases must follow established guidelines as delineated on the procurement services website.

(13) Exceptions to this policy may be considered when consistent with the goals established by rule 3356-01.01 of the Administrative Code (university policy 3356-01.01, "Supplier diversity").

3356-3-01 Purchasing.

Responsible Division/Office:	Procurement Services
Responsible Officer:	VP for Finance and Business Operations
Revision History:	June 1998; June 2001; March 2007; May 2010; January 2012; December 2016; June 2017; June 2022; March 2023
Board Committee:	Finance and Facilities
Effective Date:	~~**June 23, 2022**~~**March 2, 2023**
Next Review:	~~2027~~2028

(A) Policy statement. Employees who are delegated signature authority for university accounts are authorized to make purchasing decisions for their respective areas, following applicable university procedures. In all its business practices, the university will adhere fully to all applicable laws, regulations, and rules of the federal, state of Ohio, and local regulatory bodies. Those conducting business for the university will seek to obtain the best value when making purchases, while protecting the interests of Youngstown state university (university).

(B) Purpose. This policy helps ensure compliance with applicable federal and state purchasing regulations and provides a means for purchasing at a reasonable cost.

(C) Definitions.

(1) "Goods" are defined as, but not limited to, equipment, materials, other tangible assets, and insurance, but excluding real property or an interest in real property.

(2) "Services" are defined as any deliverable resulting from labor performed specifically for the university, whether from the application of physical or intellectual skills. Services include repair work, consulting, maintenance, data processing, and software design. Services do not include services furnished pursuant to employment agreements.

(3) "Professional design services" are defined as, but not limited to, services within the scope of practice of a state-registered architect,

registered engineer, registered surveyor, landscape architect and interior designer. See rule 3356-4-07 of the Administrative Code (university policy 3356-4-07, "Selection of design professionals for university capital projects").

(4) "Construction renovation" is defined in rule 3356-4-15 of the Administrative Code (university policy 3356-4-15, "University construction/renovation projects").

(D) Parameters.

(1) Accountability for vendor commitment and/or the actual purchase of goods or services rests with the financial manager. All construction/renovation projects must be coordinated through the university's facilities office.

(2) Procurement services has the primary responsibility to manage and monitor the purchasing process. Authority is delegated to the Maag library to purchase items to be added to its collection.

(3) As a commitment to diversity, equity and inclusion, the university provides opportunities for socially and economically disadvantaged businesses and participates in the state of Ohio's minority business enterprise (MBE) and encouraging diversity, growth and equity (EDGE) programs.

(4) To ensure the best value and compliance with applicable federal and/or state of Ohio regulations, the university requires competitive selection for certain dollar thresholds and participates in competitively awarded governmental and group purchasing agreements.

(E) Procedures.

(1) Requests for purchases are made by using a university-approved procurement card or the online procurement requisition system.

(2) An authorized electronic requisition/purchase order for goods or services must be processed through procurement services prior to vendor commitment and/or the actual purchase except for authorized procurement card purchases. Exceptions may be made in the case of an emergency, such as, but not limited to,

unexpected building repairs that could otherwise result in catastrophic structural failure.

(3) All purchases for goods and services for which there is an existing university contract or price agreement with one or more preferred vendors must be made from those vendors. This applies regardless of payment method (purchase order, p-card, etc.). Some existing university contracts and agreements can be found on punch out catalogs on the university's online procurement system. Instances where significant cost savings can be achieved by purchasing from a vendor not on an existing university contract or price agreement requires approval by the director of procurement services, or designee, prior to vendor commitment and/or actual purchase.

(4) If there is no existing university contract available, procurement services can assist in locating an approved competitively awarded governmental or group purchasing agreement, such as state term schedule, general services administration schedule, inter-university council purchasing group, or others.

(5) Competitive selection dollar thresholds.

(a) Goods or services when an individual transaction/project from a single supplier is fifty thousand dollars or more.

(b) Professional design services when an individual transaction is fifty thousand dollars or more.

(c) A construction/renovation project when the construction project cost is two hundred fifteen thousand dollars or more or the threshold established by rule 153:1-9-01 of the Administrative Code.

(6) For purchases below the competitive selection dollar thresholds, the director of procurement services, or designee, may require a minimum of three quotes or a competitive selection process when in the best interest of the university to do so or when regulations require.

(7) For purchases at or above the competitive selection dollar thresholds, appropriate forms of competitive selection include:

(a) An invitation to bid (ITB). A formal ITB is drafted and sent to prospective bidders and published in appropriate media when seeking to purchase goods.

(b) A request for proposal (RFP). RFPs are managed and distributed through the university's procurement services office. An RFP is drafted and sent to prospective bidders and published in appropriate media when seeking to purchase goods.

(c) A request for qualifications (RFQ). With the assistance of procurement services, an RFQ is sent to prospective bidders and may be published in appropriate media when seeking to purchase services. RFQs for professional design services are handled solely through the facilities office.

(d) Purchases under an approved competitively awarded governmental or group purchasing agreement, such as state term schedule, general services administration (GSA) schedule, inter-university council purchasing group, or others, some of which can be found on punch out catalogs on the university's online procurement system (eCUBE).

(8) Exceptions to competitive selection requirements.

(a) Maintenance contracts purchased from the manufacturer or authorized dealer/supplier of the specific equipment to be serviced.

(b) Software/hardware for system upgrades and ongoing maintenance and support on existing systems already in use.

(c) Special circumstances, including single source provider, emergency purchases, or economic efficacy. If the purchase is at or above the competitive selection dollar threshold and the nature of the purchase is such that competitive selection would be impractical, the department making the request for a purchase may submit a written request for a waiver of competitive selection. Such requests must include justification as to why a waiver is

warranted, be signed by the appropriate financial manager with signature authority, and be attached electronically to the requisition being submitted for the purchase.

If the director of procurement services, or designee, finds that sufficient justification has been presented, the waiver may be approved. If the director, or designee, feels that a bid waiver should be denied, it will be forwarded to the vice president for finance and business operations, or designee, for a final determination. If the request is denied, procurement services will initiate a competitive selection process at the request of the department end user.

(9) Bidding thresholds may be adjusted to comply with federal and/or state regulations.

(10) Contract compliance and administration processes will be conducted in accordance with rule 3356-3-04 of the Administrative Code (university policy 3356-3-04, "Contract compliance and administration").

(11) The university assumes no obligation for any purchases made outside of the purchasing procedures established herein. Staff who fail to follow approved processes may be subject to personal financial liability and appropriate disciplinary action.

(12) Purchases must follow established guidelines as delineated on the procurement services website.

(13) Exceptions to this policy may be considered when consistent with the goals established by rule 3356-01.01 of the Administrative Code (university policy 3356-01.01, "Supplier diversity").

YOUNGSTOWN STATE UNIVERSITY

Explanation of policy modification:

3356-4-09 Acceptable Use of University Technology Resources

Revising Acceptable Use policy to limit TikTok and other social media platforms that harvest device and/or network data to designated devices and bans use of these platforms on University owned devices that comingle data.

The revisions also provide an exception for acceptable business and academic use cases. Once an exception is granted by the CIO, the department will need to purchase a designated device where data will not be comingled.

Board of Trustees Meeting
March 2, 2023
YR 2023-

YOUNGSTOWN STATE UNIVERSITY

RESOLUTION TO MODIFY
ACCEPTABLE USE OF UNIVERSITY TECHNOLOGY RESOURCES POLICY, 3356-4-09

WHEREAS, University Policies are being reviewed and reconceptualized on an ongoing basis; and

WHEREAS, this process can result in the modification of existing policies, the creation of new policies, or the deletion of policies no longer needed; and

WHEREAS, action is required by the Board of Trustees prior to replacing and/or implementing modified or newly created policies, or to rescind existing policies.

NOW, THEREFORE, BE IT RESOLVED, that the Board of Trustees of Youngstown State University does hereby approve the modification of the University Policy stated above and attached hereto.

Board of Trustees Meeting
March 2, 2023
YR 2023-

3356-4-09 Acceptable use of university technology resources.

Responsible Division/Office:	Information Technology Services
Responsible Officer:	VP for Finance and Business Operations
Revision History:	August 1999; November 2010; December 2012; March 2016; June 2021; March 2023
Board Committee:	Finance and Facilities
Effective Date:	**March 2, 2023**
Next Review:	2028

(A) Policy statement. University technology resources are provided to the university community to support its academic and administrative functions in accordance with its teaching, research, and service missions. These resources are intended to be used for the educational and business purposes of the university in compliance with this policy.

(B) Scope. This policy applies to all users and uses of university-owned technology resources (including those acquired through grant processes) as well as to any non-YSU and/or remote technology devices while connected to the YSU network.

(C) Parameters.

(1) Technology resources (computing, digital recordings, networking, data and network services) are provided to the university community in order to fulfill the mission of the university.

(2) While the university recognizes the importance of academic freedom and freedom of expression, as a public employer, the university also has a responsibility to comply with all federal and state laws and regulations, as well as the obligation to fulfill its mission.

(3) Use of university-owned technology to access resources other than those supporting the academic, administrative, educational, research and services missions of the university or for more than limited, responsible personal use conforming to this policy is prohibited.

(4) Technology resources provided by the university are the property of the university. University-owned technology is not intended to supersede the need for technology purchases for personal purposes.

(5) As the university is a public entity, information in an electronic form may also be subject to disclosure under the Ohio public records act to the same extent as if they existed on paper. All use is subject to the identification of each individual using technology resources (authentication).

(6) Use of technology is subject to the requirements of legal and ethical behavior and is intended to promote a productive educational and work environment.

(D) User requirements. All users of the university-owned technology resources (computing, digital recordings, networking and data), regardless of affiliation with the university, must:

(1) Use only those technology resources that they are authorized to use and use them only in the manner and to the extent authorized.

(2) Protect the confidentiality, integrity and availability of technology resources.

(3) Comply with all federal, Ohio, and other applicable law as well as applicable regulations, contracts, and licenses.

(4) Comply with all applicable policies at Youngstown state university (YSU).

(5) Respect the right of other technology users to be free from harassment or intimidation.

(6) Respect copyrights, intellectual property rights, and ownership of files and passwords.

(7) Respect the privacy of other users and their accounts, regardless of whether those accounts are securely protected.

(8) Respect the finite capacity of technology resources and limit use so as not to consume an unreasonable amount of or abuse those

resources or to interfere unreasonably with the activity of other users or to disrupt the authorized activities of the university.

(9) Limit personal use of university technology resources so that such use does not interfere with one's responsibilities to the university.

(10) Not attempt to circumvent information technology security systems or the university "IT Security Manual."

(11) Not use any radio spectrum space on any YSU-owned or YSU-occupied property, unless it is part of an approved wireless services deployment by the university.

(12) Not use technology resources for personal commercial purposes or for personal financial or other gain unless specifically approved by the university.

(13) Not state or imply that they speak on behalf of the university without authorization to do so and not use university trademarks and logos without authorization to do so.

(E) User responsibilities.

(1) By accepting employment, being admitted as a student, or asking for any guest technology resource privileges, users implicitly agree to adhere to this policy and agree to adhere to the university "IT Security Manual."

(2) Users are responsible for any activity performed using their usernames and passwords except when account security is compromised by actions beyond the user's control.

(3) Users are responsible for any activity performed on university-owned technology devices assigned to them except when the device is compromised by actions beyond the user's control.

(4) There is no expectation of personal privacy when using university resources. See paragraph (F) of this rule.

(5) Potential violations regarding use of technology resources should be reported to the appropriate information technology services

manager(s) or information security officer.

(6) Users are responsible for ensuring that critical data are backed up and available to be restored for systems not administered by information systems technology. This includes critical information contained on technology devices oriented to individual use (e.g., desktops, laptops, smart phones, and similar such devices).

(7) Users are responsible for maintaining data in compliance with the university records retention plan.

(8) Users are responsible for ensuring that sensitive information to which they have access is guarded against theft. (See university policy 3356-4-13, "Sensitive information/information security"; rule 3356-4-13 of the Administrative Code.)

(9) Personal use of computing resources not otherwise addressed in this policy or these procedures will generally be permitted if such use does not consume a significant amount of resources, does not interfere with the performance of an individual's job or other university responsibilities, and is otherwise in compliance with university policies.

(F) No expectation of privacy.

(1) The university does not routinely monitor specific individual end-user usage of its technology resources. However, the university does routinely monitor technology resource usage in the normal operation and maintenance of the university's computing, network and data resources. This monitoring includes the caching and backing up of data and communications, the logging of activity, the monitoring of general usage patterns, the scanning of systems and networks for anomalies and vulnerabilities, the filtering of malicious traffic, and other activities that are necessary for the rapid and efficient delivery of services. Technology users should be aware that there is no expectation of privacy associated with the use of university technology resources.

(2) When authorized by the office of the general counsel, the university may also specifically monitor the activity and accounts of individual end-users of university technology resources,

including login sessions, file systems, and communications.

(3) When authorized by the appropriate university administrator (president, vice president, or associate vice president reporting to the president), the university may access active end-user accounts, files, or communications used for university business when needed by a supervisor or assigned personnel for university business and the end-user is unavailable. For inactive end-users, such as retirees or terminated employees, the end-user's former supervisor or the individual currently holding the supervisor position may request access. For inactive student end-users the provost may authorize access. For all other inactive end-users, the general counsel may authorize access.

(4) The university, in its discretion, may disclose the results of any such general or individual monitoring, including the contents and records of individual communications, to appropriate university personnel, student conduct, or law enforcement agencies and may use those results in appropriate university disciplinary proceedings.

(5) Personal computing devices:

(a) Personal computing devices (laptops, desktops, tablets, cellular phones) are restricted to the campus wireless network or the residence hall network.

(b) No personal computing devices will be allowed to connect to the wired campus network (excluding the residence hall network).

(c) Personal computing devices must comply with university "IT Security Manual" when using the campus wireless network or other provided university technology resource.

(d) Personal computing devices used to conduct university business are subject to public records requests.

(e) Personal hubs, routers, switches, or wireless access points are prohibited from being connected to either the university's wired or wireless network.

(G) Email. Email is an official means for communication at the university. Students, faculty, and staff are expected to check their official email address on a frequent and consistent basis in order to stay current with university communications.

(H) Security. The university employs various measures (i.e., the university's "IT Security Manual") to protect the security of information technology resources and user accounts; however, users should be aware that the university cannot provide good security without user participation. Users should increase their technology security awareness and fully employ access restrictions for their accounts, including using strong passwords, guarding passwords diligently and changing passwords regularly to help safeguard their use of technology.

Special procedures exist and must be followed to ensure that accounts for employees are secured with passwords known to only the account holder. Passwords may be changed at the request of the area supervisor and approved by the supervisor's vice president or the president.

(I) Additional policy ramifications. Users must abide by all applicable restrictions, whether or not they are built into the computing system, network or information resources and whether or not they can be circumvented by technical or other means. Individuals who engage in electronic communications with persons in other states or countries or on other systems or networks may also be subject to the laws of those states and countries and the rules and policies of those technology systems and information resources.

(J) Examples of unacceptable use:

(1) As a further aid to policy compliance, the following non-exhaustive list is provided of activities that are prohibited.

(a) Using technology resources to engage in fraud, defamatory, abusive, unethical, indecent, obscene, pornographic and/or unlawful activities is prohibited.

(b) Using technology resources to procure, solicit, or transmit material that is in violation of sexual, racial or other harassment or hostile workplace laws is prohibited.

(c) Any form of harassment by electronic means (e.g., email, videoconferencing, web access, phone, paging), whether through language, content, frequency or size of messages is prohibited. (Refer to university policies 3356-2-03, "Discrimination/harassment," 3356-2-05, "Title IX sexual harassment policy," and 3356-4-21, "Campus free speech"; rules 3356-2-03, 3356-2-05, and 3356-4-21 of the Administrative Code.)

(d) Making fraudulent offers of products, items or services using any university technology resource is prohibited.

(e) Using technology resources for unauthorized or inappropriate financial gain, unauthorized solicitation, or activities associated with a for-profit business, or engaging in an activity that involves a conflict of interest. (Refer to university policies 3356-7-01, "Conflicts of interest and conflicts of commitment" and 3356-7-19, "Access to campus for purposes of commercial solicitation or advertising"; rules 3356-7-01 and 3356-7-19 of the Administrative Code.)

(f) Creating or forwarding chain letters, Ponzi, or other pyramid schemes is prohibited.

(g) Broadcasting of unsolicited mail or messages is prohibited. Examples include chain letters, virus hoaxes, spam mail, and other email schemes that may cause excessive network traffic. Sending large numbers of electronic mail messages for official university purposes necessitates following the university's procedures for the electronic distribution of information.

(h) Sending junk mail or advertising material to individuals who did not specifically request such material (email spam) is prohibited.

(i) Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including but not limited to, the installation or distribution of pirated or other

software products that are not appropriately licensed is prohibited.

(j) Unauthorized copying and downloading of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music and films and the installation of any copyrighted software for which an active license has not been procured is prohibited.

(k) Circumventing user authentication or security of any host, network or account is prohibited. This includes, but is not limited to, monitoring by use of keylogging or session logging.

(l) Revealing your account password to others or allowing use of your account by others is prohibited. This prohibition extends to family, other household members, friends and/or co-workers.

(m) Attempting to log onto another user's account (secured or otherwise) is prohibited.

(n) Sending electronic communications in such a way that masks the source or makes it appear to come from another source is prohibited.

(o) Personal use beyond limited responsible use is prohibited.

(p) Digital recordings of any sensitive nature, such as manager-employee personnel discussions/interactions or any discussions that email sensitive or protected data (i.e., FERPA, HIPAA, etc.), as well as recording of any meeting or conversation without full disclosure that the interaction is being recorded. All recordings become subject to the public records law of Ohio, university policy 3356-9-07, "Public records" and 3356-9-09, "Records management" (rules 3356-9-07 and 3356-9-09 of the Administrative Code).

(q) Use of TikTok, or any other social media application that

freely harvests device and/or network data, is prohibited on YSU-owned devices.

(2) Under no circumstances is an employee of Youngstown state university authorized to engage in any activity that is unethical or illegal under local, state or federal law while utilizing university-owned resources.

(K) Enforcement.

(1) The office of the chief information officer (CIO) may suspend and/or restrict either an individual's or a device's access to the university network resource if:

(a) It is deemed necessary to maintain the security or functionality of the network resource.

(b) It is deemed necessary to protect the university from potential liability.

(c) The account, system, or device is believed to have been either compromised or is in violation of this policy.

(2) The office of the CIO must immediately report the enforcement action and the justification for the action to the vice president of student affairs, vice president for finance and administration, or provost (or their designee), as applicable. The university may permanently suspend all technology access of anyone using the university network resource until due process has been completed by student conduct, employee administrative discipline and/or law enforcement agencies.

(L) Exceptions.

(1) The chief information officer, or designee, may approve exceptions to this policy on a case-by-case basis (with written authorization according to the university "IT Security Manual").

(2) Faculty and staff who have a legitimate business or academic case for using TikTok or other prohibited applications can request an exception.

(a) Approved exceptions require a departmental purchase of a dedicated YSU-owned device that does not comingle university data.

3356-4-09 Acceptable use of university technology resources.

Responsible Division/Office:	Information Technology Services
Responsible Officer:	VP for Finance and Business Operations
Revision History:	August 1999; November 2010; December 2012; March 2016; June 2021; March 2023
Board Committee:	Finance and Facilities
Effective Date:	~~**June 3, 2021**~~**March 2, 2023**
Next Review:	~~2026~~2028

(A) Policy statement. University technology resources are provided to the university community to support its academic and administrative functions in accordance with its teaching, research, and service missions. These resources are intended to be used for the educational and business purposes of the university in compliance with this policy.

(B) Scope. This policy applies to all users and uses of university-owned technology resources (including those acquired through grant processes) as well as to any non-YSU and/or remote technology devices while connected to the YSU network.

(C) Parameters.

(1) Technology resources (computing, digital recordings, networking, data and network services) are provided to the university community in order to fulfill the mission of the university.

(2) While the university recognizes the importance of academic freedom and freedom of expression, as a public employer, the university also has a responsibility to comply with all federal and state laws and regulations, as well as the obligation to fulfill its mission.

(3) Use of university-owned technology to access resources other than those supporting the academic, administrative, educational, research and services missions of the university or for more than limited, responsible personal use conforming to this policy is prohibited.

(4) Technology resources provided by the university are the property of the university. University-owned technology is not intended to supersede the need for technology purchases for personal purposes.

(5) As the university is a public entity, information in an electronic form may also be subject to disclosure under the Ohio public records act to the same extent as if they existed on paper. All use is subject to the identification of each individual using technology resources (authentication).

(6) Use of technology is subject to the requirements of legal and ethical behavior and is intended to promote a productive educational and work environment.

(D) User requirements. All users of the university-owned technology resources (computing, digital recordings, networking and data), regardless of affiliation with the university, must:

(1) Use only those technology resources that they are authorized to use and use them only in the manner and to the extent authorized.

(2) Protect the confidentiality, integrity and availability of technology resources.

(3) Comply with all federal, Ohio, and other applicable law as well as applicable regulations, contracts, and licenses.

(4) Comply with all applicable policies at Youngstown state university ("YSU").

(5) Respect the right of other technology users to be free from harassment or intimidation.

(6) Respect copyrights, intellectual property rights, and ownership of files and passwords.

(7) Respect the privacy of other users and their accounts, regardless of whether those accounts are securely protected.

(8) Respect the finite capacity of technology resources and limit use so as not to consume an unreasonable amount of or abuse those

resources or to interfere unreasonably with the activity of other users or to disrupt the authorized activities of the university.

(9) Limit personal use of university technology resources so that such use does not interfere with one's responsibilities to the university.

(10) Not attempt to circumvent information technology security systems or the university "IT Security Manual."

(11) Not use any radio spectrum space on any YSU-owned or YSU-occupied property, unless it is part of an approved wireless services deployment by the university.

(12) Not use technology resources for personal commercial purposes or for personal financial or other gain unless specifically approved by the university.

(13) Not state or imply that they speak on behalf of the university without authorization to do so and not use university trademarks and logos without authorization to do so.

(E) User responsibilities.

(1) By accepting employment, being admitted as a student, or asking for any guest technology resource privileges, users implicitly agree to adhere to this policy and agree to adhere to the university "IT Security Manual."

(2) Users are responsible for any activity performed using their usernames and passwords except when account security is compromised by actions beyond the user's control.

(3) Users are responsible for any activity performed on university-owned technology devices assigned to them except when the device is compromised by actions beyond the user's control.

(4) There is no expectation of personal privacy when using university resources. See paragraph (F) of this rule.

(5) Potential violations regarding use of technology resources should be reported to the appropriate information technology services

manager(s) or information security officer.

(6) Users are responsible for ensuring that critical data are backed up and available to be restored for systems not administered by information systems technology. This includes critical information contained on technology devices oriented to individual use (e.g., desktops, laptops, smart phones, and similar such devices).

(7) Users are responsible for maintaining data in compliance with the university records retention plan.

(8) Users are responsible for ensuring that sensitive information to which they have access is guarded against theft. (See university policy 3356-4-13, "Sensitive information/information security"; rule 3356-4-13 of the Administrative Code.)

(9) Personal use of computing resources not otherwise addressed in this policy or these procedures will generally be permitted if such use does not consume a significant amount of resources, does not interfere with the performance of an individual's job or other university responsibilities, and is otherwise in compliance with university policies.

(F) No expectation of privacy.

(1) The university does not routinely monitor specific individual end-user usage of its technology resources. However, the university does routinely monitor technology resource usage in the normal operation and maintenance of the university's computing, network and data resources. This monitoring includes the caching and backing up of data and communications, the logging of activity, the monitoring of general usage patterns, the scanning of systems and networks for anomalies and vulnerabilities, the filtering of malicious traffic, and other activities that are necessary for the rapid and efficient delivery of services. Technology users should be aware that there is no expectation of privacy associated with the use of university technology resources.

(2) When authorized by the office of the general counsel, the university may also specifically monitor the activity and accounts of individual end-users of university technology resources,

including login sessions, file systems, and communications.

(3) When authorized by the appropriate university administrator (president, vice president, or associate vice president reporting to the president), the university may access active end-user accounts, files, or communications used for university business when needed by a supervisor or assigned personnel for university business and the end-user is unavailable. For inactive end-users, such as retirees or terminated employees, the end-user's former supervisor or the individual currently holding the supervisor position may request access. For inactive student end-users the provost may authorize access. For all other inactive end-users, the general counsel may authorize access.

(4) The university, in its discretion, may disclose the results of any such general or individual monitoring, including the contents and records of individual communications, to appropriate university personnel, student conduct, or law enforcement agencies and may use those results in appropriate university disciplinary proceedings.

(5) Personal computing devices:

(a) Personal computing devices (laptops, desktops, tablets, cellular phones) are restricted to the campus wireless network or the residence hall network.

(b) No personal computing devices will be allowed to connect to the wired campus network (excluding the residence hall network).

(c) Personal computing devices must comply with university "IT Security Manual" when using the campus wireless network or other provided university technology resource.

(d) Personal computing devices used to conduct university business are subject to public records requests.

(e) Personal hubs, routers, switches, or wireless access points are prohibited from being connected to either the university's wired or wireless network.

(G) Email. Email is an official means for communication at the university. Students, faculty, and staff are expected to check their official email address on a frequent and consistent basis in order to stay current with university communications.

(H) Security. The university employs various measures (i.e., the university's "IT Security Manual") to protect the security of information technology resources and user accounts; however, users should be aware that the university cannot provide good security without user participation. Users should increase their technology security awareness and fully employ access restrictions for their accounts, including using strong passwords, guarding passwords diligently and changing passwords regularly to help safeguard their use of technology.

Special procedures exist and must be followed to ensure that accounts for employees are secured with passwords known to only the account holder. Passwords may be changed at the request of the area supervisor and approved by the supervisor's vice president or the president.

(I) Additional policy ramifications. Users must abide by all applicable restrictions, whether or not they are built into the computing system, network or information resources and whether or not they can be circumvented by technical or other means. Individuals who engage in electronic communications with persons in other states or countries or on other systems or networks may also be subject to the laws of those states and countries and the rules and policies of those technology systems and information resources.

(J) Examples of unacceptable use:

(1) As a further aid to policy compliance, the following non-exhaustive list is provided of activities that are prohibited.

(a) Using technology resources to engage in fraud, defamatory, abusive, unethical, indecent, obscene, pornographic and/or unlawful activities is prohibited.

(b) Using technology resources to procure, solicit, or transmit material that is in violation of sexual, racial or other harassment or hostile workplace laws is prohibited.

(c) Any form of harassment by electronic means (e.g., email, videoconferencing, web access, phone, paging), whether through language, content, frequency or size of messages is prohibited. (Refer to university policies 3356-2-03, "Discrimination/harassment," 3356-2-05, "Title IX sexual harassment policy," and 3356-4-21, "Campus free speech"; rules 3356-2-03, 3356-2-05, and 3356-4-21 of the Administrative Code.)

(d) Making fraudulent offers of products, items or services using any university technology resource is prohibited.

(e) Using technology resources for unauthorized or inappropriate financial gain, unauthorized solicitation, or activities associated with a for-profit business, or engaging in an activity that involves a conflict of interest. (Refer to university policies 3356-7-01, "Conflicts of interest and conflicts of commitment" and 3356-7-19, "Access to campus for purposes of commercial solicitation or advertising"; rules 3356-7-01 and 3356-7-19 of the Administrative Code.)

(f) Creating or forwarding chain letters, Ponzi, or other pyramid schemes is prohibited.

(g) Broadcasting of unsolicited mail or messages is prohibited. Examples include chain letters, virus hoaxes, spam mail, and other email schemes that may cause excessive network traffic. Sending large numbers of electronic mail messages for official university purposes necessitates following the university's procedures for the electronic distribution of information.

(h) Sending junk mail or advertising material to individuals who did not specifically request such material (email spam) is prohibited.

(i) Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including but not limited to, the installation or distribution of pirated or other

software products that are not appropriately licensed is prohibited.

(j) Unauthorized copying and downloading of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music and films and the installation of any copyrighted software for which an active license has not been procured is prohibited.

(k) Circumventing user authentication or security of any host, network or account is prohibited. This includes, but is not limited to, monitoring by use of keylogging or session logging.

(l) Revealing your account password to others or allowing use of your account by others is prohibited. This prohibition extends to family, other household members, friends and/or co-workers.

(m) Attempting to log onto another user's account (secured or otherwise) is prohibited.

(n) Sending electronic communications in such a way that masks the source or makes it appear to come from another source is prohibited.

(o) Personal use beyond limited responsible use is prohibited.

(p) Digital recordings of any sensitive nature, such as manager-employee personnel discussions/interactions or any discussions that email sensitive or protected data (i.e., FERPA, HIPAA, etc.), as well as recording of any meeting or conversation without full disclosure that the interaction is being recorded. All recordings become subject to the public records law of Ohio, university policy 3356-9-07, "Public records" and 3356-9-09, "Records management" (rules 3356-9-07 and 3356-9-09 of the Administrative Code).

(q) Use of TikTok, or any other social media application that

freely harvests device and/or network data, is prohibited on YSU-owned devices.

~~(2) Exemptions. Individual university staff may be exempted from these restrictions on a case-by-case basis (with written authorization according to the university "IT Security Manual") in the course of performing legitimate job responsibilities.~~

~~(3) Passwords. Special procedures exist and must be followed to ensure that accounts for employees are secured with passwords known to only the account holder. Passwords may be changed at the request of the area supervisor and approved by the supervisor's vice president or the president.~~

~~(4)~~(2) Under no circumstances is an employee of Youngstown state university authorized to engage in any activity that is unethical or illegal under local, state or federal law while utilizing university-owned resources.

(K) Enforcement.

(1) The office of the chief information officer (CIO) may suspend and/or restrict either an individual's or a device's access to the university network resource if:

(a) It is deemed necessary to maintain the security or functionality of the network resource.

(b) It is deemed necessary to protect the university from potential liability.

(c) The account, system, or device is believed to have been either compromised or is in violation of this policy.

(2) The office of the CIO must immediately report the enforcement action and the justification for the action to the vice president of student affairs, vice president for finance and administration, or provost (or their designee), as applicable. The university may permanently suspend all technology access of anyone using the university network resource until due process has been completed by student conduct, employee administrative discipline and/or law enforcement agencies.

(L) Exceptions.

(1) The chief information officer, or designee, may approve exceptions to this policy on a case-by-case basis (with written authorization according to the university "IT Security Manual").

(2) Faculty and staff who have a legitimate business or academic case for using TikTok or other prohibited applications can request an exception.

(a) Approved exceptions require a departmental purchase of a dedicated YSU-owned device that does not comingle university data.

YOUNGSTOWN STATE UNIVERSITY

RESOLUTION TO APPROVE AN INCREASE TO THE INTERNATIONAL APPLICATION FEE

WHEREAS, Ohio law provides that Boards of Trustees of state-assisted institutions of higher education shall supplement state subsidies by income from charges to students, including an "instructional fee" for educational and associated operational support of the institution and a "general fee" for non-instructional services, and that these two fees shall encompass all charges for services assessed uniformly to all enrolled students and shall be identified as "tuition"; and

WHEREAS, Ohio law also provides that each Board may establish special purpose fees, service and housing charges, fines and penalties and that a tuition surcharge shall be paid by all students who are not residents of Ohio; and

WHEREAS, Ohio law provides that fees charged for instruction shall not be considered to be a price for service but shall be considered to be an integral part of the state government financing program in support of higher education opportunity for students;

NOW, THEREFORE, BE IT RESOLVED, that the Youngstown State University Board of Trustees does hereby approve an adjustment to the application fee for international applicants, as depicted on Exhibit A and made part hereof, effective retroactively on February 1, 2023.

Board of Trustees Meeting
March 2, 2023
YR 2023-

Exhibit A

	Current Rate	Proposed Rate	Change
International Application Fee	$45.00	$75.00	$30.00

YOUNGSTOWN STATE UNIVERSITY
General Fund and Auxiliary Enterprises
Budget to Actual and Actual to Actual Comparison
2nd Quarter (July 1 thru December 31)

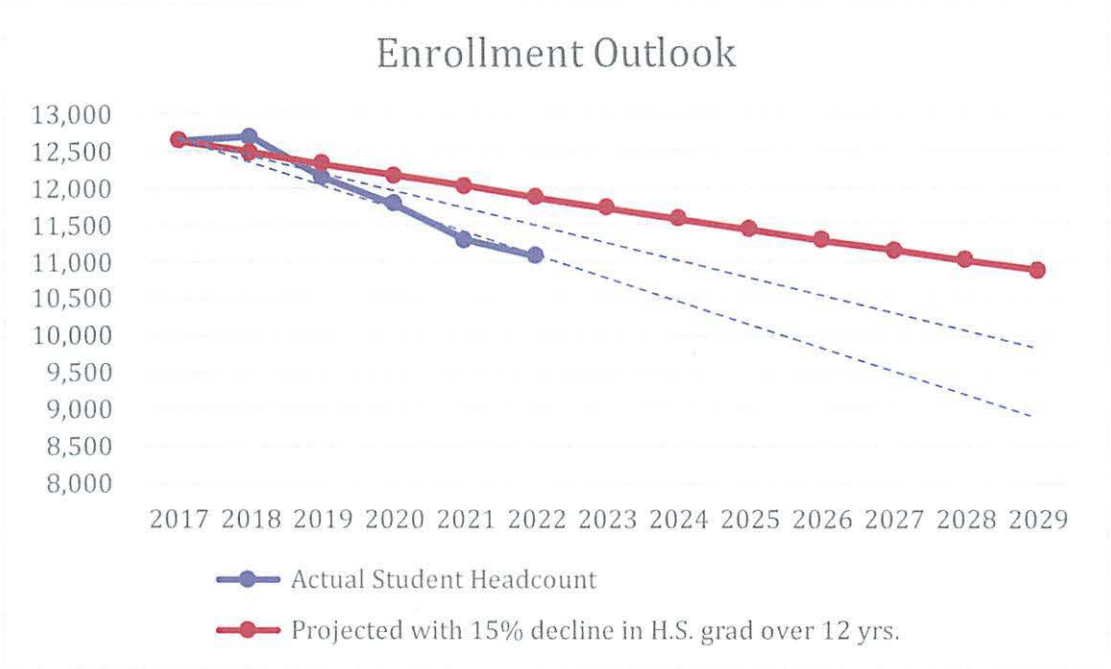
Revenue	Fiscal Year 2023		Actual as a % of Budget	Business Indicator
	Budget	Actual		
Tuition and mandatory fees	$ 89,120,575	$ 83,649,201	93.9%	●
Other tuition and fees	10,590,539	7,963,426	75.2%	●
Student charges	1,171,150	625,527	53.4%	●
State appropriations	46,588,505	23,198,158	49.8%	●
Recovery of indirect costs	1,842,813	1,166,892	63.3%	●
Investment income	2,068,718	1,129,570	54.6%	●
Other income	917,700	507,779	55.3%	●
Auxiliary enterprises	17,304,541	15,501,677	89.6%	●
Total	**$ 169,604,541**	**$ 133,742,230**	**78.9%**	●

● On/Above target
● Caution
● Warning

Expenses	Fiscal Year 2023		Actual as a % of Budget	Business Indicator
	Budget	Actual		
Wages	$ 80,392,632	$ 38,135,309	47.4%	●
Benefits	29,966,865	17,202,846	57.4%	●
Scholarships	16,294,927	12,282,793	75.4%	●
Operations	32,524,681	17,418,400	53.6%	●
Plant & maintenance	13,324,371	6,613,091	49.6%	●
Fixed asset purchases	1,182,088	298,810	25.3%	●
Transfers	(2,043,819)	903,497	-44.2%	●
Total	**$ 171,641,745**	**$ 92,854,746**	**54.1%**	●

● On/Below target
● Caution
● Warning

YOUNGSTOWN STATE UNIVERSITY



YSU Capital Projects Summary:

Board Projects Update 2/6/2023

Projects in Progress:

Utility Distribution Upgrades/Expansion
YSU 2122-07

$1.65M (Capital Funds) GPD Group, Marucci Gaffney
This project is mostly complete with few items remaining.

Watson Team Center
YSU 2122-19

$1.9M (Gift/Philanthropy Funds) YSU Staff, Murphy Contracting
Work is complete but awaiting final building inspections and approvals for occupancy.

Stambaugh Classroom/Beeghly Physical Therapy
YSU 2122-15

$1.5M (Local Funds) OSPORTS, Hudson Construction
Stambaugh is essentially complete, but HVAC equipment has still not arrived. Beeghly Center moving forward for a March completion.

Projects Out for Bids:

- Arlington Parking Facility, Bids due February 15th at 2:00pm

Projects at Controlling Board for Release of Funds:

- RAPIDS Grant equipment

Request for Architect/Engineer Qualifications Advertisements:

- None at this time.

Projects in Development for 2023:

Elevator Safety Repairs and Replacements
YSU 2122-08

$550k (Capital Funds) Domokur, Murphy Contracting
Phase 2 of last year's project will include the full upgrade of the elevator and equipment in Silvestri Hall. Additionally, water infiltration issues will be addressed in the Beeghly Center elevator.

Moser Hall Renovations Phase 2
YSU 2122-21

$900k (Capital Funds) YSU Staff
A continuation of last year's project that will address Schwebel Auditorium.

Arlington Parking Facility
YSU 2324-11

$800k (Local Funds) GPD Group
This project will create a parking facility on Arlington and Fifth Avenue, at the location of the demolished M60 parking deck. This project will be completed this Summer.

Lyden Restrooms Phase 2
YSU 2324-20

$600k (Local Funds) Olsavsky-Jaminet, Brock Builders
The second phase of a project that will completely upgrade restroom facilities in Lyden House dorm. This project will be completed this summer.

Campus Roof Replacements YSU 2324-02	***$2M (Capital Funds) Prime AE Group*** This project will replace sections of the roofs on Cushwa Hall and the Edmund J. Salata Complex. This project will start this summer and be complete in the Fall.
Garfield Building Renovations Phase 1 YSU 2324-15	***$800k (Capital Funds) Prime AE Group*** This project will replace the roof on the Garfield Building. Construction will start late Fall 2023 or early Spring 2024 depending on material availability.
Emergency Generator Upgrades YSU 2324-19	***$1M (Capital Funds) YSU Staff*** This project will upgrade and replace emergency generators across campus. Construction will start Summer of 2023 and will be complete by Fall.
STEM Science Lab Renovations YSU 2324-13	***$800k (Capital Funds) YSU Staff*** This project will renovate STEM labs on the 5th and 6th floors of Ward Beecher. New flooring, ceilings, lighting, paint, and furniture upgrades are planned. This project will start in May 2023 and will be complete for the start of Fall Semester.

Additional Projects in Development:

- **Cafaro Hall, Cafaro Suite Renovations** – Upgrades to room finishes and furniture.
- **M30 Deck Maintenance** – Annual preventative maintenance on the M30 parking deck.
- **Lyden House Elevator Design** – Developing a design for the Lyden House elevator replacement.
- **Building Envelope Renovations** – Doors, windows, and brick/stone exteriors will be repaired/replaced.
- **Maag Library Learning Commons** – Renovate areas within the Maag Library to accommodate the relocation of the Resch Academic Success Center and Accessibility Services.

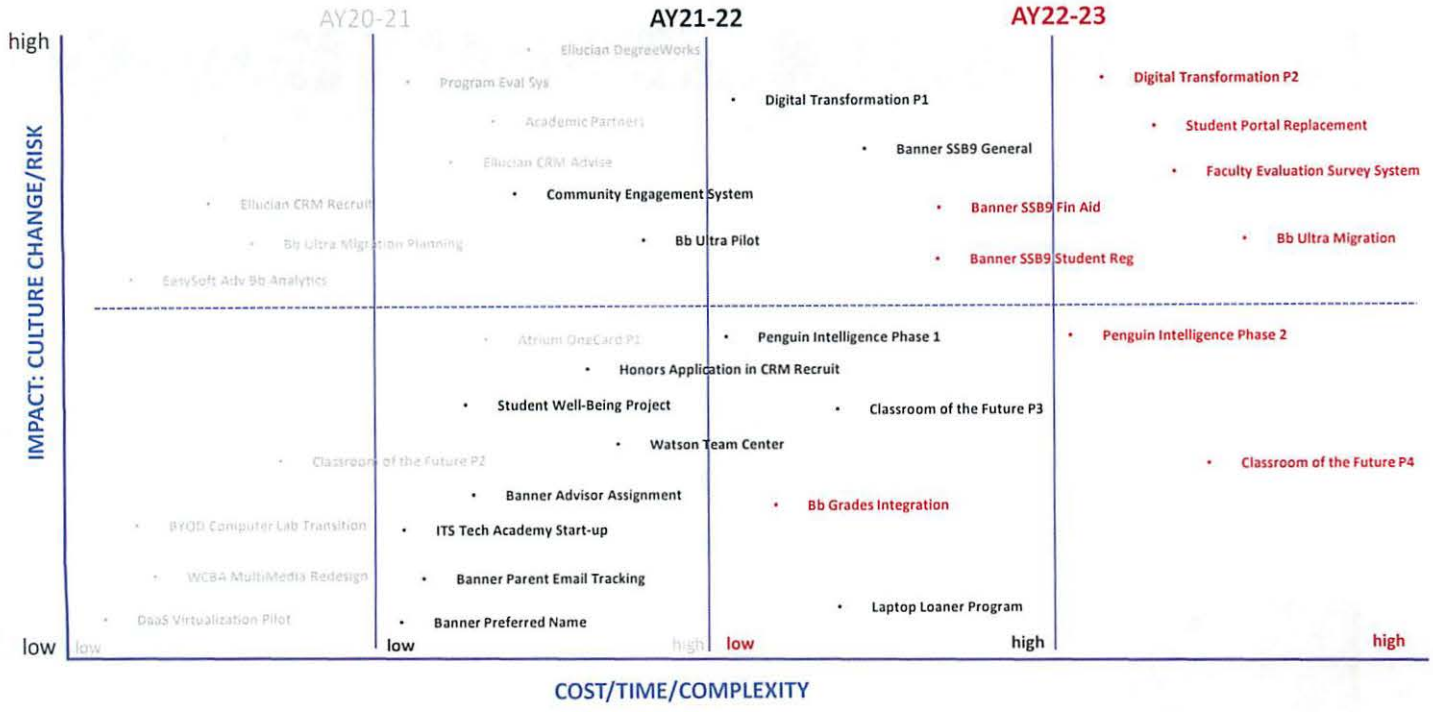
Information Technology Services Update

Board of Trustees
March 2023

YOUNGSTOWN STATE UNIVERSITY

AY20-21 thru AY22-23 Technological Innovation for Strategic Transformation

Student Success & Experience Technology-enabled Initiatives



ITS Key Performance Indicators (KPI'S) Summary

2022 Annual Update

Department	KPI	KPI Measure	Annual Evaluation (2022)	Comments
ITS - Overall	1	ITS Productivity	82%	80% benchmark achieved; Administrative (i.e. meetings, paperwork, etc.) < 20%. Looking to raise benchmark to 85%.
Customer Services**	2	CSAT Campus Survey Quality of Service *(n=343)*	76.0%	YSU App Cloud dissatisfaction by Engineering students dominated negative responses.
	3	Ticket Survey *(n= 1,917)* *Faculty & Staff (96%) *Students (93%)	94%	Survey completed post ticket closure. *Most accurate measure of satisfaction.*
Infrastructure Services	4	Uptime - Wi-Fi	99.4%	Downtime primarily due to a firmware release upgrade glitch causing multiple reboots of controllers.
Training Services	5	Growth %	226%	'21 to '22: Workshops, Consultations & Participants Increased an average of 226% combined

**According to the American Customer Satisfaction Index, A CSAT Benchmark of very satisfied and satisfied is >77%. (Green); Average- 70-76% (Yellow) and below 70% (Red) Considered critical and needs immediate attention.

ITS Security Key Risk Indicator (KRI's) Summary

2022 Annual Update

Department	KPI	KRI Measure	Annual Evaluation (2022)	Comments
Security Services	1	Operating System Compliance	81.8%	Windows devices are highly compliant (nearly 100%). Apple devices will be focus through the remainder of this year. Current Apple OS compliance = 70%.
	2	Endpoint Point Protection	100%	Endpoint protection installed and maintained on every YSU-owned device (Security best-practice)
	3	Threat Landscape (last 30 days)	99.9%	a) Malicious emails blocked; Out of 23669 of 23693 email, 24 were manually remediated during that time frame b) 156,250 Firewall threats blocked c) 440k attempts to compromise were against our approximate 106k accounts; 4 confirmed compromised accounts, 1 semi-successful breach

YOUNGSTOWN STATE UNIVERSITY

YSU IT Major Projects

Department	Project	Project Name	Health	Comments
Project Management Office	1	Penguin Intelligence – Student Module Implementation		Resource constraints/availability have delayed this implementation. New target June.
	2	Data Integrity Initiative		On hold due to demands of SSB9 projects; Slated for April start.
	3	Watson Team Center		Complete
	4	Blackboard Ultra Course & Grades Syllabus Initiative		Blackboard Ultra – Fall 2024
	5	Ellucian-NeoEd Talent Management System Implementation		Target - 5/8/23
	6	Banner Majors and Concentrations Revamp		Target - 3/31/23

YOUNGSTOWN STATE UNIVERSITY

YSU IT Major Projects

Department	Project	Project Name	Health	Comments
Project Management Office	7	Banner SSB-9 Financial Aid		Complete
	8	Watermark Faculty Evaluations Surveys		Complete; Historical survey data is being reformatted for input to the Watermark system.
	9	Luminis Portal Replacement Project		Target – 9/1/24
	10	Banner SSB-9 Student Registration		Target – 3/1/23
	11	Penguin Intelligence HR/Finance modules		Target - 6/30/23
	12	Banner SSB-9 HR/Payroll		Target – 6/30/23

YOUNGSTOWN STATE UNIVERSITY

Thank you!

YOUNGSTOWN
STATE
UNIVERSITY