HIGHLAND COMMUNITY COLLEGE
District #519

AGENDA
Board of Trustees Meeting
May 21, 2024 – 4:00 p.m.
Robert J. Rimington Board Room (H-228)
Highland Community College Student/Conference Center
Freeport, Illinois

Public access to the meeting is provided online via
https://highland.zoom.us/j/88320472535?pwd=SmdzVjE3cDRVenFIaFBYRm5sV2VlQT09
or by phone at 312-626-6799 using meeting ID 883 2047 2535 and Passcode 643643

I. Call to Order/Roll Call

II. Approval of Trustee(s) Attending Meeting Via Electronic Means

III. Approval of Agenda

IV. Approval of Minutes: April 30, 2024 Regular Meeting

V. Public Comments

VI. Introductions

VII. Budget Report

VIII. Foundation Report

IX. Consent Items

A. Academic (None)

B. Administration (None)

C. Personnel

1. Part-time Instructors, Overload, and Other Assignments (Page 1)

D. Financial (None)

X. Main Motions

A. Academic (None)

B. Administration

1. First Reading – Revised Policy 1.111: Board Member Attendance by a Means Other Than Physical Presence (Page 3)
2. First Reading – New Policy 3.072: Medical Withdraw (Page 5)
3. First Reading – New Policy 3.40: Disability Services Documentation (Page 7)
4. First Reading – Revised Policy 5.23: Technology Acceptable Use (Page 9)
5. First Reading – New Policy 5.231: Password Controls (Page 17)
6. First Reading – Revised Policy Appendix: Information Technology Acceptable Use Guidelines (Page 20)

7. Real Estate Donation Agreement Between Highland Community College and the Highland Community College Foundation for Use by the Highland Community College Agriculture Department (Page 29)

C. Personnel

1. Appointment: Nursing Instructor (Page 31)
2. Appointment: College Access Specialist, TRIO Educational Opportunity Centers (EOC) (Grant Funded) (Page 32)
3. Appointment: Head Coach/Coordinator, Athletic Compliance (Page 33)
4. New Job Description: Career Services Specialist (Page 34)
5. New Job Description: Manufacturing Mentor/Coach (Grant Funded) (Page 37)
6. Revised Job Description: Student Success Coach (Grant Funded) (Page 40)
7. Acceptance of Staff Member Requesting to Participate in the Planned Retirement Program (Page 44)

D. Financial

1. Change Order with Interact Communications for General Marketing Media Buy/Digital Advertising (Page 45)
2. Course Fee Change for Spring 2025 (Page 48)
3. Auditor for Fiscal Year 2024 (Page 49)
4. Memorandum of Understanding with Transformative Community Health for Campus Based Mental Health Services (Page 62)
5. Purchase of Copiers and Printers from Marco Technologies, LLC, and Related Maintenance (Page 76)
6. Payment of Bills and Agency Fund Report – April 2024 (Page 80)

XI. Reports

A. Treasurer's Report: Statements of Revenue, Expenditures, and Changes in Fund Balance (Page 82)

B. Student Trustee

C. Audit and Finance Committee

D. Illinois Community College Trustees Association (ICCTA) Representative

E. Association of Community College Trustees (ACCT)

F. Board Chair

G. President

XII. CLOSED SESSION

A. Appointment, Employment, Compensation, Discipline, Performance, or Dismissal of Specific Employees of the Public Body or Legal Counsel for the Public Body

B. Collective Negotiating Matters

XIII. ACTION, IF NECESSARY

A. Appointment, Employment, Compensation, Discipline, Performance, or Dismissal of Specific Employees of the Public Body or Legal Counsel for the Public Body

1. Appointment: Vice President/Chief Academic Officer (CAO), Academic Services (Handout)

B. Collective Negotiating Matters

XIV. Old Business

XV. New Business

XVI. Dates of Importance

A. Next Quarterly Board Retreat – June 25, 2024 at 1:00 p.m. in the Robert J. Rimington Board Room (H-228)

B. Budget Work Session – July 16, 2024 at 3:00 p.m. in the Robert J. Rimington Board Room (H-228)

C. Next Regular Board Meeting – July 16, 2024 at 4:00 p.m. in the Robert J. Rimington Board Room (H-228)

XVII. Adjournment

AGENDA ITEM #IX-C-1
MAY 21, 2024
HIGHLAND COMMUNITY COLLEGE BOARD

PART-TIME INSTRUCTORS, OVERLOAD, AND OTHER ASSIGNMENTS

RECOMMENDATION OF THE PRESIDENT: That the attached list of part-time instructors, overload and other assignments be approved.

BACKGROUND: The individuals listed have been certified by the hiring supervisor as having the required training and experience to perform duties or teach courses offered by Highland Community College. Each course is contingent upon appropriate enrollment.

BOARD ACTION: _____

Spring 2024				COURSE	CLOCK	CREDIT		TOTAL
FIRST	LAST	CRN	SUBJECT	TITLE	HRS	HRS	RATE	SALARY
Lifelong Learning								
Tari	Heap	6737	PERS036	De-Stressing in Turbulent Times		1	$25.00	$25.00
Cindy	Bielefeldt	6754	PERS036	Resin Jewelry		4		$120.00
Mark	Peterson	6745	PERS036	WWII in Europe Overview		1.5	$27.50	$41.25
Roger	Hicks	6726	PERS036	Welding for Garden Art - Bug		3		$322.00
Dana	Russell-Brown	6706	PERS036	Intermediate Wheel-Thrown Pottery		8	$25.00	$200.00
Dale	Anderson	6705	PERS036	Metal Detecting Basics		2	$25.00	$50.00
Mark	Peterson	6725	PERS036	Civilian Conservation Corps		1.5	$27.50	$41.25
Science/Math								
Amanda	Lessman	6465	NURS109BXH	Basic Nursing Assistant		2.55	$1,397.43	$3,563.45
Constance	Taylor			Curriculum Assignment for Freeport Middle School Students		3	$28.09	$84.27
Crystal	Winters	6464	NURS109BXH	Basic Nursing Assistant Lab		11	$38.00	$418.00

Other Assignments			
John	Hartman	Piano tuning	$ 325.00
Emily	Stich	Transposed Trombone parts for Hindesmith piece	$ 50.00
Taylor	Griffin	Light Board operator for Carl Cole event	$ 52.50
Elijah	Michael	Stage Manager for Carl Cole event	$ 52.50
Annette	Hartman	HCC billboards, Stephenson County Fair billboard adjustments, signage for parade vehicles	$ 1,020.00
Ella	Caswell	Instrumentalist in the Spring Choral concert	$ 175.00
Hannah	Caswell	Instrumentalist in the Spring Choral concert	$ 150.00
Laura	Caswell	Instrumentalist in the Spring Choral concert	$ 150.00
Lynn	Kaufman	LifeLong Learning instructor	$ 512.00
Austin	Rickels	Keynote speaker for HCC Leadership conference	$ 400.00

AGENDA ITEM #X-B-1
MAY 21, 2024
HIGHLAND COMMUNITY COLLEGE BOARD

FIRST READING – REVISED POLICY 1.111 BOARD MEMBER ATTENDANCE BY A MEANS OTHER THAN PHYSICAL PRESENCE

RECOMMENDATION OF THE PRESIDENT: That the Board of Trustees approves for first reading revised policy 1.111, Board Member Attendance by a Means Other Than Physical Presence, which is included in Chapter I, Board of Trustees, of the policy manual.

BACKGROUND: The Illinois Open Meetings Act (5 ILCS 120/7) was recently updated to include that a member of a public body may now attend a meeting by means other than in person (i.e., video or audio conference) due to unexpected childcare obligations. In order for the Board to permit a trustee to attend electronically due to unexpected childcare obligations, the policy must be updated to include this reason.

BOARD ACTION: _____

1.111 *Board Member Attendance by a Means Other Than Physical Presence*
(Adopted)

In accordance with the Illinois Open Meetings Act [5 ILCS 120/7], Board members may be permitted to attend, participate, and vote at meetings by telephone conference call or other electronic means under the following conditions:

A. If a quorum of Board members is physically present at a Board meeting, a majority of the Board may vote to allow a Board member who is not physically present to attend the meeting by other means (i.e., video or audio conference) if the member is prevented from physically attending because of:

   1. personal illness or disability;
   2. employment purposes or the business of the College; ~~or~~
   3. a family or other emergency; or
   ~~3.~~4. unexpected childcare obligations.~~.~~

B. If a Board member wishes to attend a meeting by other means, the Board member must notify the Board Secretary of the College before the meeting unless advance notice is impractical.

AGENDA ITEM #X-B-2
MAY 21, 2024
HIGHLAND COMMUNITY COLLEGE BOARD

FIRST READING – NEW POLICY 3.072 MEDICAL WITHDRAW

RECOMMENDATION OF THE PRESIDENT: That the Board of Trustees approves for first reading new policy 3.072, Medical Withdraw, which is proposed for inclusion in Chapter III, Student, of the policy manual.

BACKGROUND: This policy outlines the process and requirements for students to request a medical withdrawal from their classes due to an extended medical or family emergency. This is a longstanding procedure and is recommended to be placed in the policy manual to ensure the process is documented and accessible.

BOARD ACTION: _____

3.072 Medical Withdraw (Adopted)

Students who are unable to participate in their classes for an extended period of time due to a medical or family emergency may request a medical withdraw. Requests for medical withdraws should be made to the director of enrollment and records through a written request explaining the circumstances accompanied by documentation from a physician or medical institution to verify the medical condition, date of onset, and estimated length of treatment that interferes with attending and completing classes and assignments. Retroactive withdraws will be considered until the end of the fall or spring semester following the semester for which the medical/administrative withdraw is being requested.

Students granted a medical withdraw may receive a grade of AW (Administrative Withdrawal) which carries no academic penalty and is not used in the calculation of the student's grade point average. Administrative Withdraw is considered for all courses in a given semester and is not usually granted for select courses. Students will receive written notification of the decision from the Admissions and Records Office.

AGENDA ITEM #X-B-3
MAY 21, 2024
HIGHLAND COMMUNITY COLLEGE BOARD

FIRST READING – NEW POLICY 3.40
DISABILITY SERVICES DOCUMENTATION

RECOMMENDATION OF THE PRESIDENT: That the Board of Trustees approves for first reading new policy 3.40, Disability Services Documentation, which is proposed for inclusion in Chapter III, Student, of the policy manual.

BACKGROUND: This policy is required by the Removing Barriers to Higher Education Success Act and is effective immediately.

BOARD ACTION: _____

3.40 Disability Services Documentation (Adopted)

In accordance with 110 ILCS195/1 Removing Barriers to Higher Education Success Act, documentation of disability is required of all students registering with Disability Services at Highland Community College. It is the responsibility of the student to provide information which verifies their condition meets the definition of a disability as defined by laws such as Section 504 of the Rehabilitation Act of 1973, the Americans with Disabilities Act of 1990, and the ADAAA of 2008. Student accommodation requests for disability services and accommodations will be considered on an individual, case-by-case basis through an interactive process. The College will determine if the recommendations are reasonable and appropriate for each student. In accordance with federal and state law, additional documentation may be required as outlined in the procedural handbook. Disability documentation is maintained by Disability Services separate from academic records.

The following documentation is sufficient to establish that an enrolled or admitted student is an individual with a disability:

- Documentation of an Individualized Education Program (IEP) in effect immediately prior to exiting high school.
- Documentation of services or accommodations provided under a Section 504 Plan provided to the individual pursuant to Section 504 immediately prior to exiting high school.
- Documentation of a plan or record of service from a private school, a local educational agency (LEA), a State educational agency, or an institution of higher education provided under a Section 504 plan.
- A record or evaluation from a relevant licensed professional finding that the individual has a disability.
- A plan or record of disability from another institution of higher education.
- Documentation of a disability due to military service in the uniformed services.

AGENDA ITEM #X-B-4
MAY 21, 2024
HIGHLAND COMMUNITY COLLEGE BOARD

FIRST READING – REVISED POLICY 5.23 TECHNOLOGY ACCEPTABLE USE

RECOMMENDATION OF THE PRESIDENT: That the Board of Trustees approves for first reading revised policy 5.23, Technology Acceptable Use, which is included in Chapter IV, Finance and Facilities, of the policy manual.

BACKGROUND: The recommended changes address regulatory and audit requirements for the inclusion of technology use and security provisions in College policy. This language has been updated and transferred from the policy Appendix Information Technology Services Acceptable Use Guidelines to be included in a more succinct and easily identifiable location.

BOARD ACTION: _____

5.23 *Technology Acceptable Use (Revised)*

A. Scope:

1. This policy defines the acceptable use of computing resources owned, operated, and managed by Highland Community College. This policy applies to all persons accessing or using Highland's technology resources, including all employees, students, affiliates, volunteers, or visitors at the College, hereafter referred to as users. This policy is included in the Student Code of Conduct.

B. Policy:

1. In order to promote excellent information and network security posture for Highland Community College, users must comply with institutional and external standards for appropriate use, whether on campus or from remote locations.

2. The purpose of this policy is to outline the acceptable use of computing resources and any information maintained in any form and any medium within the College's computing resources and explain violations of acceptable use. Additionally, all creation, processing, communication, distribution, storage, and disposal of information by any combination of college resources and non-college resources are covered by this policy, which supplements all applicable College policies, including harassment, patent and copyright, student and employee disciplinary policies, and FERPA, as well as applicable federal and state laws.

3. Highland Community College values the privacy rights of all individuals using its computing resources. As a usual business practice, Highland does not routinely monitor individual usage of its computing resources. Nonetheless, users should be aware that all computing resources are the property of Highland. As such, the college may access and monitor computing resources and any information stored on or transmitted through those computing resources, for legitimate business purposes including, but not limited to, system monitoring and maintenance, complying with legal requirements, police investigations, investigating security incidents, and administering this or other Highland policies. Further, to protect systems on the Highland network, the college may, without prior notice if deemed necessary, remove compromised devices from the network, block malicious traffic from entering the network, and prohibit devices within Highland's network from connecting to known malicious outside entities.

C. User Accounts:

1. The use of Highland's computer systems and network requires that the College issue a user account. Every computer user account issued by Highland is the responsibility of the person whose name it is issued. Users are responsible for any activity originating from their accounts that which they can reasonably be expected to control.

Under any circumstances, accounts and passwords may not be used by persons other than those to whom the Highland Network Administrator has assigned them. In cases when unauthorized use of accounts or resources is detected or suspected, the account owner should change the password and report the incident.

2. College recognized clubs and student organizations may be issued a user account. Club advisors shall designate a particular person(s) (e.g., club president) authorized to act on behalf of the club or organization. This person(s) is responsible for all activity on the account and will be subject to College disciplinary procedures for misuse.

3. The college employs various measures to protect the security of its computing resources and its user's accounts. Users should be aware, however, that the college cannot guarantee security and confidentiality. Users should therefore engage in "safe computing" practices using long complex passphrases, employing Multi-Factor Authentication, and guarding their passwords and MFA methods.

D. User Responsibilities:

Users of Highland Community College's technology resources have a shared responsibility with the College's Information Technology Services staff to maintain the integrity of systems, services, and information.

1. User responsibilities include:

   a. ~~To use the College's technology resources responsibly, only for college business purposes, and consistent with the terms of this policy. All college business is to be conducted on college-owned or through college contracted (delete and replace with provided?) services. User's personal activities need to use non-Highland accounts, email accounts, data storage, and devices.~~To use the College's technology resources responsibly and consistent with the terms of this policy. Users acknowledge college-owned devices and college-contracted services are to be primarily used for college business, and any incidental non-business use will be included in the college's data retention schedule and subject to college FOIA requests.

   b. To access only files and data that the user owns, that are publicly available, or to which the user has been given authorized access by the data owner.

   c. To use only legal versions of copyrighted software in compliance with vendor license agreements.

   d. To comply with College, federal, state, and local regulations regarding access and use of information resources (e.g., College policies regarding the sensitive information and dissemination of information outside the campus, Federal

Copyright Act, The Family Education Rights and Privacy Act, Gramm-Leach-Bliley Act, Red Flag, HIPAA, codes of professional responsibility, etc.).

e. To keep technology accounts (computer, network, and application) secure:
   1. Lock Highland devices when leaving unattended.
   2. ~~Do not share personal credentials or privileges with others. Access to personal technology resources is not transferable.~~ Access to technology resources is not transferable. Usernames, passwords, or privileges are not to be shared with others, unless specified in Highland's Password Policy.
   3. Report suspected unauthorized access to a supervisor or the Information Technology Services department.
   4. Allow all ITS Department software and security patches to install.

~~a.~~ f To keep all institutional data in safe-keeping. Specifically, ~~i~~information containing any personally identifiable information (PII) or data of students, staff or others should not leave the institution in a digitally unsecured method and should always be stored on the college's ~~network (H: and G:)~~ storage drives.

g. To ensure digital content is compliant with other College policies, copyright laws, and applicable local, state, federal laws (including, but not limited to: Americans with Disabilities Act and Web Content Accessibility Guidelines 2.0). Published digital content is not to be used for commercial purposes or for activities not related to the purposes of the College, without written authorization from the College.

h. To inform the ITS department when planning for a new service, or when changing an existing college service or function. The only exceptions are if the service or function do not, in any way, interface with technology.

i. No user shall seek to hold Highland Community College liable for damage resulting from unauthorized interception, use, misuse, damage or destruction of information resources. Each authorized user shall hold Highland Community College harmless and indemnify it for any expense or loss caused by their own unauthorized interception, use, misuse, damage, or destruction of information resources, or by their violation of this policy.

2. Violations of this Policy include, but are not limited to:

   a. Illegal Use - Using computing resources to upload, download, transmit, post, or store any material or data that, intentionally or unintentionally, violates any applicable local, state, national or international law, or violates the rules, policies, or procedures of the College or any college department is prohibited. Transmitting, uploading, downloading, or storing any material that infringes upon an existing copyright, trademark, patent, trade secret, or other legal right using

computing resources is also prohibited.

b. Threats or Harassment - Using computing resources to transmit material or data that causes or encourages physical or intellectual abuse, damage, or destruction of property, or that knowingly causes or encourages harassment, explicit or implied, is prohibited.

c. Transferring of Use – Permission to use computing resources is granted to individuals and may not be transferred to others. Sharing of a personal username/password assigned to an individual is expressly prohibited. Use of another user's ID or seeking to access another user's account is prohibited. Similarly, individuals may not use their user credentials to provide access to Highland's wireless network to other individuals. The following will be considered theft of services.

1. Acquiring a username in another person's name.
2. Using a username without the explicit permission of the owner and Information Technology Services.
3. Allowing one's username to be used by another person without the explicit permission of Highland's ITS department.
4. Using former system and access privileges after association with Highland has ended.

d. Malicious Content - Use of Highland computing and messaging systems to transmit any material which contains malicious content, such as malware or phishing scams, or any other content that may damage computer systems or collect or misuse personal information is prohibited.

e. Intercepting Communications - Using packet sniffers, password capture applications, keystroke loggers, and other tools that perform similar behavior or any form of network wiretapping on computing resources is prohibited. Using such tools to diagnose, analyze, or mitigate ongoing service issues or security violations may be permitted when conducted by authorized personnel.

f. Forgery or Impersonation - Falsifying or removing identifying information on computing resources with intent to deceive, defraud, or misguide is prohibited. Impersonation of other persons or groups with the intent to harm is prohibited. Unauthorized use of the College's registered Internet domain name(s) is also prohibited.

g. Unauthorized Access or Penetration Attempts (i.e., "hacking") - Unauthorized access or penetration attempts of Highland computing resources, or a remote entity using Highland computing resources, are prohibited. Users must not use computing resources to impair or damage the operations of any computers, networks, terminals, or peripherals.

h. Service Interruptions - Using computing resources to permit or promote activity that adversely affects the integrity or performance of computing resources is prohibited. Denial of service attacks, forged packet transmission, and similar actions may be permitted when conducted by authorized College personnel.

i. Circumvention of controls – Deliberately circumventing security controls or exploiting vulnerabilities at Highland or any other network from Highland equipment or network is prohibited. Gaining access by exceeding the limits of assigned authorization is likewise prohibited. Users shall not develop or use procedures to alter or avoid the accounting and monitoring of the use of computing facilities. For example, users may not utilize facilities anonymously or by using an alias. They may not send messages, mail, or print files that do not show the correct username of the user performing the operation.

j. Excessive or Unreasonable Use - Users shall not use information technology resources to excess. Excessive use of information technology resources by a particular user or for a particular activity reduces the amount of resources available to satisfy the needs of other users. Excessive use may degrade or jeopardize system functionality and result in significant costs to the college. Some examples of excess use may include writing a program or script or using an Internet bot to perform a repetitive task such as attempting to register for a class or purchasing event tickets online.

k. Fraudulent Activity - Using computing resources to transmit material or communications to promote a financial scam or wrongdoing is prohibited.

l. Creation, interference with, or transmission of Wireless Signals – Creation of new wireless network requires explicit permission of Highland's ITS department. Interfering with Highland's wireless networks or attaching a device to transmit a Highland network is strictly prohibited.

m. Personal Gain - Computing resources are not to be used for commercial purposes or personal financial or other gains.

n. Abuse of communication systems - Sending unsolicited messages, which in the College's judgment, is disruptive to system resources or generates a significant number of user complaints is prohibited. This includes using any college communication system (email, text, app, or phone calls) to send spam, bulk, or malicious messages, including commercial advertising, political tracts, or other inappropriate use of system distribution lists. Bulk messaging should not be the venue for any all-campus conversations.

o. Institutional Image - Unless resources are used to meet the College's purpose, to support our educational and community values, and/or to support our programs

and initiatives, users are prohibited from accessing, submitting, publishing, displaying, or posting any defamatory, inaccurate, abusive, obscene, profane, sexually oriented or explicit, threatening, racially offensive, harassing, or illegal material.

p. Abuse of incidental personal use - Incidental personal use must not:

1. Be illegal.
2. Interfere with a Highland employee's job responsibilities/work.
3. Interfere with the legitimate education and business purposes of Highland.
4. Result in any measurable cost to the College.
5. Adversely affect the availability, integrity, or reliability of Highland IT systems or cause harm to the activities of others using the IT systems.
6. Violate this policy or other College policies.
7. Be inconsistent with the College's status as a state entity and its non-profit, tax-exempt status.

q. Physical Security - Unauthorized access to, destruction, extension, or alteration of, theft, damage, or tampering of any physical computing resources, including computer workstations, kiosks, card swipes, printers, audio-visual equipment, telephone/fax equipment, classroom equipment, or wiring closets is prohibited. This applies to all network wiring, hardware, and in-room jacks. Users shall not use the network to provide Internet access to anyone outside of the College community for any purpose other than those that are in direct support of the academic mission of the College.

E. Reporting & Enforcement:

1. Violations of this Policy may be reported through one's supervisor, the Highland ITS Service Desk, or as otherwise permitted through College policy.

2. The College may, without notice, disable or suspend access to the system as part of any routine maintenance or concern over the safety and security of the system.

3. Users who violate this policy may be denied access to college computing resources and may be subject to other penalties, including financial costs, and/or disciplinary action, including possible expulsion or dismissal. Alleged violations will be handled through the college disciplinary procedures applicable to the user. The college may suspend, block, or restrict access to an account, independent of such procedures, when it reasonably appears necessary to protect the integrity, security, or functionality of college or other computing resources or to protect the college from liability. The college may also refer suspected violations of applicable law to appropriate law enforcement agencies.

4. When Highland ITS becomes aware of a possible violation, an investigation will be initiated with relevant campus offices, such as the appropriate Vice President, Human Resources, and local authorities. Users are expected to cooperate fully in such investigations when requested.

5. To prevent further unauthorized activity during such an investigation, Highland ITS may suspend authorization for the use of all computing facilities for the user(s) involved in the violation.

~~The College will provide relevant access to and use of its technology resources, including computers, communication devices, software, and information technology, in form and function suitable and appropriate for the College environment. All technology resources provided by the College are to be used in accordance with the College's Acceptable Use Guidelines. All utilization of technology resources shall be in compliance with all applicable law and regulations, and shall be in compliance with College policy, College guidelines and College procedures. The College shall take reasonable measures to protect technological resources, and to assure the technology resources are used only for their intended purposes. The College retains control and supervision of all technology resources and reserves the right to monitor the use of technology resource activity by any user. No user shall have an expectation of privacy in his or her use of technology resources, including email messages and stored files.~~

~~A. The College shall develop and implement Acceptable Use Guidelines and procedures to ensure responsible use of the technology resources, to assure the security, reliability, integrity and availability of information, and to protect technology resources against accidental or unauthorized disclosure, and against unauthorized modification or destruction. Such guidelines and procedures shall be consistent with the academic freedom rights and responsibilities of faculty members, and shall make appropriate provisions for the protection of authorized proprietary research work product produced by faculty members. The Administration and Policy Review Committee shall review the Acceptable Use Guidelines and procedures annually and shall promptly inform the Board of Trustees and the users of the technology in the event of any significant changes to the guidelines not mandated by State or Federal law.~~

~~B. Student and visitor use of computer-based technology is outlined in the Student Code of Conduct. Faculty and staff use of computer-based technology is outlined by applicable Board Policy and/or contractual language.~~

AGENDA ITEM #X-B-5
MAY 21, 2024
HIGHLAND COMMUNITY COLLEGE BOARD

FIRST READING – NEW POLICY 5.231 PASSWORD CONTROLS

RECOMMENDATION OF THE PRESIDENT: That the Board of Trustees approves for first reading new policy 5.231, Password Controls, which is proposed for inclusion in Chapter IV, Finance and Facilities, of the policy manual.

BACKGROUND: The recommended changes address regulatory and audit requirements for the inclusion of password requirements and security provisions in College policy. This language has been updated and transferred from the policy Appendix Information Technology Services Acceptable Use Guidelines to be included in a more succinct and easily identifiable location.

BOARD ACTION: _____

5.231 Password Controls (Adopted)

A. Scope:

1. This policy applies to anyone who has a Highland user account, including but not limited to: students, employees, volunteers, and consultants. This also applies to electronic devices and systems connected to the College's network including computers, network switches and routers, mobile devices, and laptop computers.

B. Policy:

1. This policy identifies the minimum password requirements needed to protect Highland Community College data and systems. The security of the College's data is highly dependent upon the secrecy and characteristics of the password. Compromised passwords can result in loss of data, denial of service for other users, or attacks directed at other Internet users from a compromised account. Compromised passwords can also result in the inappropriate disclosure of private data such as private student data, institutional data, and private employee data. To prevent unauthorized access to Highland's computer systems, users must practice proper password management. This includes:

   - Never sharing a personal Highland password with anyone. However, if ITS department supplied credentials for a shared account(s) are allocated, then only authorized users may know those credentials and their usage and storage be treated as personal credentials.
   - Never using a Highland password for personal accounts.
   - Passwords should never be written down and left in plain sight. If a password must be written down it should be stored in a secured location.
   - Passwords should never be stored electronically in plaintext. A password manager should be used to securely store passwords electronically.
   - All users must enroll their accounts in and use Multifactor Authentication (MFA) when configurable.
   - Users must secure workstations when they are away from them. Devices will be subject to lockouts for inactivity after 10 minutes.
   - Users must change their password if there is suspicion it has been compromised. Users must immediately report suspected password compromises by contacting the ITS Service Desk.
   - After multiple unsuccessful consecutive logon attempts (e.g., incorrect passwords) the user's account may become automatically locked. Users may need to contact the Service Desk for account unlocking.
   - Proper password management also applies to external hosted software used for College business. If password standards cannot be followed with a hosted service, contact the ITS Service Desk.

C. Standards:

1. Passwords must meet the following complexity requirements:
   - Must contain at least 12 characters.
   - Must contain 3 out of the following character types:
     - Uppercase letter
     - Lowercase letter
     - Number
     - Special character (e.g. !@#*&)
   - Must not contain the user's first name, middle name, last name, or username.
   - Must not match any of your recent previous passwords.

D. Reporting & Enforcement:

1. Violations of this Policy may be reported through one's supervisor, the Highland ITS Service Desk, or as otherwise permitted through College policy.

2. Users who violate this policy may be denied access to college computing resources and may be subject to other penalties and disciplinary action, including possible expulsion or dismissal. Alleged violations will be handled through the college disciplinary procedures applicable to the user. The college may suspend, block, or restrict access to an account, independent of such procedures, when it reasonably appears necessary to protect the integrity, security, or functionality of college or other computing resources or to protect the college from liability. The college may also refer suspected violations of applicable law to appropriate law enforcement agencies.

3. When Highland ITS becomes aware of a possible violation, an investigation will be initiated with relevant campus offices, such as the appropriate Vice President, Human Resources, and local authorities. Users are expected to cooperate fully in such investigations when requested.

4. To prevent further unauthorized activity during such an investigation, Highland ITS may suspend authorization for the use of all computing facilities for the user(s) involved in the violation.

AGENDA ITEM #X-B-6
MAY 21, 2024
HIGHLAND COMMUNITY COLLEGE BOARD

FIRST READING – REVISED POLICY APPENDIX INFORMATION TECHNOLOGY ACCEPTABLE USE GUIDELINES

RECOMMENDATION OF THE PRESIDENT: That the Board of Trustees approves for first reading revised policy appendix, Information Technology Services Acceptable Use Guidelines, which is included in appendix, of the policy manual.

BACKGROUND: The recommended changes address regulatory and audit requirements for the inclusion of technology use and security provisions in College policy. This language has been updated and transferred to revised policy 5.23 Technology Acceptable Use to be included in a more succinct and easily identifiable location.

BOARD ACTION: _____

Highland Community College
Information Technology Services
Acceptable Use Guidelines
Updated 2020

Highland Community College provides technology resources to meet the College's purpose, to support our educational and community values, programs and initiatives. Highland Community College's Information Technology Services organization's goal is to provide high quality services to the campus community. To ensure that our high standards are met, we have certain expectations regarding the use of technology resources at the College.

Access to Highland Community College technology resources - computing facilities, network services, servers, equipment, software, applications, information resources, printing and scanning services, and user and technical support provided by Information Technology Services staff - is a privilege, not a right. This privilege is extended to all users - faculty, staff, students, trustees, alumni/ae, affiliated individuals and organizations, partner non-profits, guests, and Pre-K-12 schools. Accepting access to this technology carries an associated expectation of responsible and acceptable use.

This "Acceptable Use Guidelines" document describes activities that Highland Community College considers acceptable use, as well as violations of use, of technology resources. The examples listed are not exhaustive and may change from time to time as technology and applications change. The examples are provided solely for guidance to users. If you are unsure whether any use or action is permitted, please contact the Director, Information Technology Services for assistance at 815-599-3480.

While there are cases in which the use of technology resources is deemed not responsible or not acceptable, there are also more serious cases in which technology resources are used in the conduct of behaviors which violate College policies, code of conduct, or local, state, or federal law. Though the use of technology resources is the focus of this document, members of the Highland Community College community and others using Highland Community College's technology resources are advised that use may also be governed by other College policies including but not limited to those in the student handbook, College catalog, and other policies governing academic, student life, or personnel matters at the College or agreements between the College and affiliated organizations. Highland Community College's technology and information resources are not to be used for commercial purposes or non-College related activities without written authorization from the officer(s) of the College that have been so designated (contact the Director, Information Technology Services for further information).

Highland Community College reserves the right to enforce applicable penalties in accordance with College policies, code of conduct, or local, state, or federal law and/or immediately terminate access to College systems and network services to any user in cases where technology resources have been used in a manner that is disruptive or is otherwise believed to be in violation of "acceptable use" or other College policies or law. The College will act in accordance with the provisions of the Digital Millennium Copyright Act in the event of notification of alleged copyright infringement by any user.

~~The College retains control, custody and supervision of all College provided computer technology. To ensure proper network performance and security, as well as appropriate use, authorized Information Technology Services staff may monitor and record user activity. No user shall have expectations of privacy in their use of computer technology, including e-mail messages and stored files.~~

~~Although Highland Community College takes measures to safeguard integrity and confidentiality, it in no way guarantees the safety or security of information resources. Highland Community College disclaims liability for the unauthorized interception, use, misuse, damage or destruction of information resources. No student, faculty member, staff member, or authorized user shall seek to hold Highland Community College liable for damage resulting from unauthorized interception, use, misuse, damage or destruction of information resources. Each authorized user shall hold Highland Community College harmless and indemnify it for any expense or loss caused by his/her own unauthorized interception, use, misuse, damage, or destruction of information resources, or by his/her violation of this Acceptable Use Guideline document.~~

~~Thousands of current and future students, faculty, staff, alumni, and donors are utilizing social media sites such as Facebook, Twitter, LinkedIn, YouTube, Instagram, Snapchat, Pinterest, and a whole host of messaging apps, blogging sites and comment interfaces to stay personally and professionally connected. HCC believes that having a presence in these areas will allow the College to broadcast information and interact with the public in ways that will further Highland's mission, vision, and core values.~~

~~Social media sites are powerful communication tools that have a significant impact on organizational and professional reputations. Because they blur the lines between personal voice and institutional voice, Highland Community College has developed guidelines, located within this document, to help clarify how best to enhance and protect personal, professional, and institutional reputations when participating in social media.~~

~~Both in professional and institutional roles, employees need to follow the same behavioral standards while participating in social media as they would in real life situations. The same College policies, Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPAA), code of conduct, professional expectations, and guidelines for interacting with students, parents, alumni, donors, media, and other constituents apply online as in face-to-face situations. Employees and students are personally accountable for anything they post to any social media sites and/or apps.~~

~~User and Staff Responsibilities:~~

~~As a user or staff member of Highland Community College's technology resources, you have a shared responsibility with the College's Information Technology Services staff to maintain the integrity of our systems, services, and information so that high quality services can be provided to everyone. Your responsibilities include:~~

1. ~~To use the College's technology resources responsibly and appropriately, respecting the rights of other users to system, services, and information access 24 hours per day, 7 days per week.~~

2. To respect all contractual and license agreements, privacy of information, and the intellectual property of others.

3. To comply with College, federal, state, and local regulations regarding access and use of information resources (e.g., College policies regarding the sensitive information and dissemination of information outside the campus, Federal Copyright Act, The Family Education Rights and Privacy Act, Gramm-Leach-Bliley Act, Red Flag, HIPAA, codes of professional responsibility, etc.).

4. To exercise due diligence in protecting any personally owned technology devices you connect to the Highland Community College wireless network from viruses, worms, and security vulnerabilities by regularly using anti-virus software.

5. To keep your technology accounts (computer, network, and application) secure. Report suspected unauthorized access to your supervisor or the Information Technology Services department.

6. To not share your privileges with others. Your access to technology resources is not transferable to another member of the Highland Community College community, to family members, or to an outside individual or organization.

7. To comply with posted policies governing use of public computing facilities.

8. To present a Highland Community College digital presence that reflects the highest standards of quality and responsibility. As the owner of digital content, you are responsible to ensure that the images, words, links, and references from your digital presence are consistent with this and other College policies, copyright laws, and applicable local, state, federal laws (including, but not limited to: Americans with Disabilities Act and Web Content Accessibility Guidelines 2.0). Published digital content is not to be used for commercial purposes or for activities not related to the purposes of the College, without written authorization from the College.

9. To understand the implications of sharing personal information or data via the Internet, e-mail, Instant Messaging or other services that either are open to access by others on and off campus, or that can be forwarded to others.

10. To keep all institutional data in safe keeping. Information containing any personal data of students, staff or others should not leave the institution unsecured.

11. To ensure all information is stored to the network (H: and G:) and not to local computer hard drives (C:).

Examples of Violations of "Acceptable Use"

Unauthorized Access Unauthorized Accounts

1. Attempting to obtain unauthorized access or circumventing user authentication or security of any host, network or account ("cracking"). This includes accessing data not intended for the

~~user, logging into a server or account the user is not expressly authorized to access, or probing the security of systems or networks.~~

~~2. Supplying or attempting to supply false or misleading information or identification in order to access Highland Community College's technology resources.~~

~~3. Sharing your passwords or authorization codes with others (computing, e-mail, applications, etc.)~~

~~4. Using technology resources for unauthorized or illegal uses.~~

~~5. Logging onto another user's account; sending e-mail, etc. from another user's account or device or from an anonymous account.~~

~~6. Unauthorized use of the College's registered Internet domain name(s).~~

~~7. Changing your Highland Community College-issued machine name to a name that is different from that assigned by Information Technology Services.~~

~~***Unauthorized Access to or Use of Services and Equipment***~~

~~8. Attempting to interfere with service to any user, host, or network. This includes "denial of service" attacks, "flooding" of networks, deliberate attempts to overload a service, port scans and attempts to "crash" a host.~~

~~9. Use of any kind of program/script/command designed to interfere with a user's computer or network session.~~

~~10. Intentionally damaging or tampering with a computer or part of a computer system.~~

~~11. Knowingly spreading computer viruses.~~

~~12. Modifying the software or hardware configuration of College technology resources, including dismantling computers in the lab for the purposes of connecting a notebook computer to the peripherals.~~

~~13. Excessive use of technology resources for "frivolous" purposes, such as game playing, streaming non-educational audio/video, or downloading files. This causes congestion of the network or may otherwise interfere with the work of others, especially those wanting to use public access PCs or network and Internet resources.~~

~~14. "Hacking" on computing and networking systems of the College or using the College's network to "hack" other networks.~~

~~15. Setting up wireless access points (WAPs).~~

~~16. Employees are not to use technology services excessively for personal use while performing their regular assigned duties.~~

17. Unless resources are used to meet the College's purpose, to support our educational and community values, and/or to support our programs and initiatives, users are prohibited from accessing, submitting, publishing, displaying, or posting any defamatory, inaccurate, abusive, obscene, profane, sexually oriented or explicit, threatening, racially offensive, harassing, or illegal material.

Unauthorized Use of Software, Data & Information

18. Inspecting, modifying, distributing, or copying software or data without proper authorization, or attempting to do so.

19. Violating software licensing provisions.

20. Installing software on College machines without appropriate authorization (from Information Technology Services).

21. Installing any diagnostic, analyzer, "sniffer," keystroke/data capture software or devices on College technology resources.

22. Breaching confidentiality agreements for software and applications; breaching confidentiality provisions for institutional or individual information.

Unauthorized Use of Email/Internet Messaging

23. Harassment or annoyance of others, whether through language, frequency or size of messages.

24. Sending unsolicited bulk mail messages ("junk mail" or "spam") which, in the College's judgment, is disruptive to system resources or generates a significant number of user complaints. This includes bulk mailing of commercial advertising, political tracts, or other inappropriate use of system e-mail distribution lists. Bulk mail should not be the venue for any all-campus conversations.

25. Forwarding or otherwise propagating chain e-mail and pyramid schemes, whether or not the recipients wish to receive such mailings. This includes chain e-mail for charitable or socially responsible causes.

26. Malicious e-mail, such as "mailbombing" or flooding a user or site with very large or numerous items of e-mail.

27. Forging of e-mail header envelope information.

28. Forging e-mail from another's account.

~~***Unauthorized Use of Highland Community College Digital Media & Servers***~~

~~29. Posting digital content that provides information on and encourages illegal activity, or is harassing and defaming to others.~~

~~30. Linking your digital presence to sites whose content violates College policies, local, state, and/or federal laws and regulations.~~

1. ~~Running a digital presence that support commercial activities or running server systems under the College's registered domain name, HIGHLAND.EDU or variation thereof, without the College's authorization.~~

Social Media Acceptable Use Guidelines ~~and Acceptable Uses~~ (reaffirmed)

A. General Posting Recommendations:

1. Be honest about your identity. If you desire to post about Highland in an unofficial capacity, please identify yourself as a Highland faculty or staff member. Never conceal your identity for the purpose of promoting Highland through social media. An excellent resource about transparency in social media sites is the Blog Council's "Disclosure Best Practices Toolkit" at http://blogcouncil.org/disclosure/

2. Be accurate in your posts. Make sure that you have all the facts before you post. It's better to verify information with a source first than to have to post a correction or retraction later. Cite and link to your sources whenever possible. If you make an error, correct it quickly and visibly. This will earn you respect in the online community.

3. Be respectful to others. You are more likely to accomplish what you want if you are positive and respectful while discussing a bad experience or disagreeing with an idea or person.

4. Be a valued member of the sites in which you are participating. If you join a social network like a Facebook group or comment on a blog, make sure you are contributing valuable input. Refrain from posting information about topics like Highland events unless you are sure it will be of interest to readers. Self-promoting behavior is viewed negatively and can lead to you being banned from certain sites or groups.

5. Take care to think before you post. There's no such thing as a "private" social media site. Search engines can turn up posts long after the publication date. Comments can be forwarded or copied. Archival systems save information even if you delete a post. If you feel annoyed or passionate about a subject, it's advisable to hold off posting until you are calm and clear-headed.

6. Maintain confidentiality at all times. Do not disclose confidential or proprietary information about Highland, its students, its alumni or your fellow employees. Use

good ethical judgment and follow College policies and federal requirements, such as FERPA and HIPAA. As a guideline, don't post anything that you would not present at a conference.

7. Respect College time and property. As stated in Section 5.23 of the College Policy Manual, computers and your work time are to be used for College-related business. It is appropriate to post at work if your comments are directly related to accomplishing college-related goals, such as seeking sources for information. You should maintain your personal sites on your own time using non-Highland devices.

B. Official Highland Community College Social Media Accounts:

To ensure that any and all interactions on behalf of Highland represent the College's best interests, the following guidelines are for those Highland employees authorized to participate and/or maintain official social media sites on behalf of the College. These guidelines are designed to be broad in nature to accommodate differences in online venues while maintaining a universal code of conduct.

1. To be recognized by the College as an official HCC social media account, the account administrator(s) must seek approval from the Community Relations (CR) office. The CR office will review all social media inquiries. This office should also be used as a resource for the college community for any social media needs. The CR Office will ensure the pages are set up properly according to the social media site's policy.

2. All Highland Community College social media accounts including, but not limited to, academic departments, student clubs and organizations, and public events, must have a HCC faculty or staff member as an administrator at all times. The CR office will have administrator privileges.

3. Should an HCC employee account administrator leave the College or no longer wish to be an account administrator, the CR office should be notified before removing him/herself from that role. College employees identified as account administrators are held responsible for managing and monitoring content of their officially recognized accounts.

4. Administrators are responsible to remove content that may violate the College's policies. If you have questions regarding the appropriateness of a post to a site that you administer, please contact the CR office.

5. Paid advertising, including but not limited to boosting, sponsoring, or promoting a post, through social media must be coordinated through the Community Relations office.

Content:

1. Use good judgment about content and respect privacy laws. Do not include confidential information about the College, its staff, or its students.

2. Do not post content that is threatening, obscene, a violation of intellectual property rights or privacy laws, or otherwise injurious or illegal.

3. Be mindful of posting personal opinions on official College social media accounts. Do not use the HCC name to promote any product, cause, or political candidate.

4. By posting content to any social media site, you agree that you own or otherwise control all of the rights to that content, that your use of the content is protected fair use, that you will not knowingly provide misleading or false information, and that you hold the College harmless for any claims resulting from the content.

5. HCC has the right to remove any content for any reason, including but not limited to, content that it deems threatening, obscene, a violation of intellectual property rights or privacy laws, or otherwise injurious or illegal.

6. When using or posting online material that includes direct or paraphrased quotes, thoughts, ideas, photos, or videos, from an outside source, always include citations. Provide a link to the original material if applicable.

7. Do not use information and/or conduct activities that may violate local, state, or federal laws, and regulations.

8. Crisis communications will be directed by the Public Information Officer and must be shared in a timely manner on all Highland Community College social media accounts including, but not limited to, academic departments, student clubs and organizations, and public events.