Pine Technical College

Policy 701 Appendix #1, Information Security Process

Pine Technical College Network Access

Network access is provisioned based on a completed System Access form. This form is located on the College Intranet. The hiring manager is responsible for completing and submitting the form to the IT department prior to the employee start date. For permanent employees, the access must be authorized by the Chief Human Resources Officer and the hiring manager. For temporary and adjunct faculty employees, only the hiring manager must authorize the access the form. An end date must be specified for all temporary and adjunct faculty employees.

Upon receipt by the IT department, the CIO will approve the request. IT department staff will create the account and prepare an information packet for the employee.

The hiring manager is also responsible for scheduling a meeting between the new employee and the CIO to review security policies and other information.

Network access is contingent on compliance with all other policies and procedures including Policy 708, Acceptable Use of Information Technology.

Administrative Network Access

Administrative access to Pine Technical College network infrastructure will be granted to IT Department staff by the Chief Information Officer based on job function. Administrative access for non-IT department staff must be requested in writing using a system access form and must be approved by the College President and the CIO prior to granting rights. Documentation must demonstrate business need, define the specific rights being requested, and the specific dates and times access is required. This includes IT specific administrative tools such as patch management, vulnerability management, etc.

Pine Technical College Email

Pine Technical College assigns email accounts to all staff if requested on the System Access form used for granting network access.

Special purpose email addresses are provisioned for a variety of uses including role based email accounts, student group accounts, and other purposes. All special purpose email accounts must be approved by the CIO. Special purpose email accounts must be requested by the manager responsible for the work unit, student club advisor, or other responsible party. The request must be submitted to the helpdesk via email.

All registered students will receive a campus email account.

The ability to send email to the list of all students is controlled. Only individuals with a documented business need will be granted the right to send email to all students. Requests to create a group or modify group membership must be made via email to the helpdesk by the member of the Manager's Group responsible for the individual seeking access.

Email distribution groups are maintained by the IT Department. Requests to create or modify a distribution group must be submitted to the IT department via an email to the helpdesk. All requests will be reviewed by IT staff prior to creating or modifying the group.

Email system resources such as rooms, vehicles, AV equipment, etc. are established by the IT department and assigned an owner who is responsible for maintaining the calendar for the individual resource. Requests to provision an email system resource must be submitted to the IT department via an email to the helpdesk. All requests will be reviewed by IT staff prior to provisioning the resource.

Shared File Storage

Pine Technical College assigns shared file storage to staff if requested on the System Access form used for granting network access.

Shared file storage is maintained by the IT Department. Only individuals with a documented business need will be granted rights to share file storage. Requests to create or modify access to a shared file store must be made via email to the helpdesk by the supervisor of the individual seeking access. All requests will be reviewed by IT staff prior to creating or modifying shared file storage access.

Shared file storage is maintained for students. All students are granted read-only access to the store. Faculty members are granted read/write access to individual folders within the student shared storage upon request. Requests must be submitted to the helpdesk via email by the faculty seeking access.

ISRS

Overview, The College President appoints the CIO to fill the Security Director role. Security Director approves individual role managers. Role managers are responsible for approving individual user right requests for their business areas. System HR approval is also required for all HR rights requests. All rights and roles must be reviewed annually. This system is maintained by the System Office.

All users must complete the Public Jobs: Private Data training prior to receiving ISRS rights.

ISRS can only be accessed from the staff workstations.

Financial Aid: EdConnect, EdExpress, and various web applications

Access to EdConnect and EdExpress are managed by the Financial Aid Director by the authority granted by the Department of Education. Access to the financial aid modules are managed in accordance to the ISRS access section above. Financial aid also access several state, federal, and other websites to perform business functions. Access to these sites is granted by the Financial Aid Director's supervisor or the College President or through affiliation with the Department of Education. See appendix 2 for details.

US Department of Education access rights are granted by updating the Eligibility and Certification Approval Report (ECAR) with the name of the individual seeking access. The ECAR shows compliance with the US Department of Education Program Participation Agreement (PPA). The updated report is submitted to the US Department of Education for approval. Signature of the College President and Chief

Financial Officer is required. When the application is approved, an updated ECAR with a copy of the College's PPA is sent to the College. Financial Aid Director, Chief Financial Officer, and College President have administrative rights for granting access to U.S. Department of Education websites for department staff.

Right Now

Requests to access to the Right Now application must be submitted by the supervisor of the individual seeking access by an email to the helpdesk or through the use of a Systems Access form. All requests will be reviewed by IT staff prior to granting or modifying access.

MN Pals

The Campus Library Director, referenced by MnPALs as the Systems Librarian, controls security and access to protected processes and operations for the ALEPH (ExLibris) automated library system. The Systems Librarian grants access to and privileges for the automation modules in which the college currently participates to other library staff members. The Systems Librarian determines which privileges (operational functions) other staff members may use based on business need. Access to each module requires a special user name and password. Access to MnPALS' training manuals, support documentation for the Aleph System, and Help Desk are protected by a secured log-in. Only two non-public staff workstations can be utilized for Aleph services and administration.

The PALS Office in Mankato has the information and authority to grant rights for the Aleph System to each college's Systems Librarian and to do so in the case of an emergency and/or change in local personnel.

Operational Data: Replicated Data, Hyperion/Brio

Access to Operational Data is obtained by submitting an Operational Data Security Request Form to the Office of the Chancellor. The Office of the Chancellor maintains the official record. This form requires signature approval from the users immediate supervisor, the signature authorities for each module requested, the campus Security Director/CIO, and, in the case of HR data the campus CHRO and Office of the Chancellor HR approval. Access to Replicated Data is restricted to the CAP server. Access to Hyperion/Brio is restricted to the CAP server and staff workstations.

CAP Server

Access to the Cap server is a two-step process. First, the individual requesting access to the CAP server must be granted rights to MnSCU Operational Data through the approved process. Second, access to the CAP server must be requested through the use of a System Access form or via an email to the helpdesk initiated by the supervisor of the individual seeking rights. A copy of the approved Operational Data Security form must be attached to the request. IT staff will configure the access to the CAP server based on the request. Access to the CAP server is restricted to individual workstations as well as individual users. Access to the CAP server is only available through appropriately configured staff workstations. Supervisors are responsible for reviewing Operational Data Security and notifying the Helpdesk of any changes via email during the reauthorization process each December.

Hall Displays

Hall display access is managed by the Marketing department. All requests for display access must be submitted to the Director of Marketing who will approve the request and submit a copy to the IT Department for processing. Request for use of hall display areas may be submitted by any member of staff or faculty.

Website edit/admin

Approval to administer services or publish content to the college website is controlled by the college's Director of Marketing and Admissions and/or the College CIO. Access to the College website must be requested via an email to the helpdesk initiated by the supervisor of the individual seeking rights. The Marketing Director or College CIO will review the request and reply with their approval. IT staff will create an account within the content management system. The college webmaster will review the user database annually and take appropriate action.

Image Now

Access to ImageNow is managed by the PTCC ImageNow Administrators (Lisa Hosna and Shawn Reynolds). Access requests must be submitted to the PTCC ImageNow Administrators via email by the supervisor of the individual seeking rights. The PTCC ImageNow Administrators will review the access request to ensure business justification as well as appropriate separation of duties. Once reviewed, the PTCC ImageNow Administrators will grant access within the ImageNow system. The PTCC ImageNow Administrators will rescind or adjust the rights of specific users upon notice of position change or separation. The PTCC ImageNow Administrators will review all user rights and roles annually and take appropriate action.

SEMA4/Swift/State IA Warehouse

Access to State of Minnesota mainframes and other resources are managed by the appropriate state agency. Information regarding access to State Applications can be found on the MnSCU website (http://its.mnscu.edu/security/securityforms/stateofmnsystems/index.html). Supervisors of staff accessing State applications and services are responsible for following the appropriate procedures.

Pine Technical College

DARS

Workforce One

TrackDat

Maxis/Blue Zone

MBS

QuickBooks (Foundation)

MAPS

Online Banking

Document Direct (??)

(CCA?)

Remote access to academic applications (e.g. automotive databases)

Desire2Learn

Blumen

Neogov

Academic Alert

Accuplacer

End of program assessment tools

Background check tools

Resumix

Pine Technical College

Additional information provided by MnSCU Office of the Chancellor

Basic Security Access for MnSCU HR Staff

The following information details how to request access to the applications and reporting tools that are used by MnSCU HR staff.

Mainframe logon ID –

Complete the form and fax to the number at the bottom of the form (612.626.5450). You will receive email notification from MnSCU ITS with logon ID and temporary password. This logon ID is required for access to SEMA4, MAPS, Document Direct, and IA Warehouse

Request for SEMA4 Security Access –

Complete this form after you have been assigned a Mainframe Logon ID. The form should be signed by the employee and the employee's supervisor. Fax the form to Barb Biljan at OOC (651.297.3145) for the *Signature Agency Security Administrator*

Request for Access to Document Direct On-Line Reports –

Complete this form after you have been assigned a Mainframe Login ID. Fax the form to Barb Biljan at OOC (651.297.3145) for the *Signature Agency Security Administrator*

Operational Data Security Request Form (Access to Hyperion/BRIO)

This form should be signed by the employee and the employee's supervisor. Fax the form to ITS Security (651.917.4731). ITS Security will follow up if additional signatures are required

SCUPPS/ISRS

Using the Web Based Security Application, an employee can request access which is then approved at the campus level by the Campus Approval Manager. Multi-Campus Requests must be approved by Office of the Chancellor

Tuition Waiver

Using the Web Based Security App, employee can request access which is approved at the campus level by the Campus Approval Manager. Multi-Campus Requests must be approved by Office of the Chancellor

Pine Technical College

Financial Aid Application Access

Description	Agency	Access Approved By
Student Aid Internet Gateway (used to set up enrollment and several of the sites below): https://fsawebenroll.ed.gov/PMEnroll/index.jsp	US Department of Education	College President via PPA
Common Origination & Disbursement Website: https://www.cod.ed.gov/cod/LoginPage	US Department of Education	College President via PPA
Financial Aid Administer Access to Central Processing Center: http://www.fafsa.ed.gov/FOTWWebApp/faa/faa.jsp	US Department of Education	College President via PPA
National Student Loan Data Center: https://www.nslds.ed.gov/nslds_FAP/secure/logon.jsp	US Department of Education	College President via PPA
VA Once for Certifying VA Benefits: https://vaonce.vba.va.gov/vaonce_student/default.asp	Department of Veterans Affairs	Dean or Student Affairs
MN State Grant Access: https://www.ohe.state.mn.us/SSL/SG/index.cfm	MN Office of Higher Education	Dean or Student Affairs
Child Care Grant / Workstudy Reporting: https://www.ohe.state.mn.us/ssl/cc_ws_eoy/index.cfm	MN Office of Higher Education	Dean or Student Affairs
MN Indian Scholarship / MN GI Bill / MN Achieve Scholarship: https://www.ohe.state.mn.us/SSL/FAApp/default.aspx	MN Office of Higher Education	Dean or Student Affairs
FFELP Loan Process via Great Lakes: https://www.mygreatlakes.org/	Great Lakes Guarantor Agency	Dean or Student Affairs
Firstmark Servicing for SELF Loans: https://www.firstmarkservices.com/index.aspx?ReturnUrl=%2fDefault.aspx	FirstMark and MN Office of Higher Education	Dean or Student Affairs
E-Campus Based System (FISAP): https://cbfisap.ed.gov/ecb/CBSWebApp/	US Department of Education	College President via PPA
E-App used to update our Program Participation Agreement: http://www.eligcert.ed.gov/	US Department of Education	College President via PPA
Older Direct Loan website, still used for some functions, but is being phased out: https://schools.dl.ed.gov/schools/school/index.do	US Department of Education	College President via PPA