Information Technology

Department

Policies and Procedures Manual

Overview

This document serves as a rulebook and roadmap for successfully and properly utilizing the technology resources at Imperial Valley College (IVC). Careful consideration should be taken to verify that one's actions fall within the authorized parameters for access, utilization, distribution, and modification of IVC's technology resources set forth within this document.

Any misuse, misappropriation, negligence, or deliberate disobedience concerning these policies and procedures will not be tolerated. It is up to each individual employee and affiliate of IVC to familiarize him/herself with the policies and procedures set forth herein prior to signing the agreement form at the end of this document.

It is the purpose of the IVC Information Technology (IT) Department to provide these policies and procedures in order to address potential situations and to provide steps to take during these situations. However, not all situations can ever be addressed so it is up to each individual employee and affiliate to use these policies and procedures for an example of what type of actions to take.

The IVC IT Department does encourage all IVC employees and associates to err on the side of caution should a difficult situation present itself that is not discussed herein. If this should occur, the employee or associate of IVC can always take advantage of the IVC IT Department's open-door policy and ask for assistance.

Contents

Policies

Acceptable Use Policy

Overview

This policy establishes the acceptable usage guidelines for all IVC-owned technology resources. These resources can include, but are not limited to, the following equipment:

- Computers
  - Desktop Computers, Mobile Devices, Servers, etc.
- Network Equipment
  - Switches, Routers, Network and Communications Cabling, Wall Plates, Wireless Antennas, Wireless Bridge Devices, Fiber Optic Lines, Fiber Optic Equipment, VoIP Phones, etc.
- Audio/Video Equipment
  - Video Codecs, HDTVs, Document Cameras, Projectors, Security Cameras, Miscellaneous Cabling, Digital Cameras and Camcorders, Printers, Copiers, Fax Machines, etc.
- Software
  - Operating Systems, Application Software, etc.
- Resources
  - Group Drive File Storage, Website File Storage, Email Accounts, Social Networking Accounts, etc.

This policy applies to all employees, contractors, consultants, temporaries, and other workers at IVC, including any and all personnel affiliated with third parties, including vendors. This policy applies to all equipment that is owned or leased by IVC.

Policy

The District computer and network systems are the sole property of Imperial Community College District. They may not be used by any person without the proper authorization of the District. The Computer and Network systems are for District instructional and work related purposes only.

This procedure applies to all District students, faculty and staff and to others granted use of District information resources. This procedure refers to all District information resources whether individually controlled or shared, stand-alone or networked. It applies to all computer and computer communication facilities owned, leased, operated, or contracted by the District. This includes personal computers, workstations, mainframes, minicomputers, and associated peripherals, software and information resources, regardless of whether used for administration, research, teaching or other purposes.

Conditions of Use

Individual units within the District may define additional conditions of use for information resources under their control. These statements must be consistent with this overall procedure but may provide additional detail, guidelines or restrictions.

Legal Process

This procedure exists within the framework of the District Board Policy and state and federal laws. A user of District information resources who is found to have violated any of these policies will be subject to disciplinary action up to and including but not limited to loss of information resources privileges; disciplinary suspension or termination from employment or expulsion; and/or civil or criminal legal action.

Copyrights and Licenses
Computer users must respect copyrights and licenses to software and other on-line information.

Copying – Software protected by copyright may not be copied except as expressly permitted by the owner of the copyright or otherwise permitted by copyright law. Protected software may not be copied into, from, or by any District facility or system, except pursuant to a valid license or as otherwise permitted by copyright law.

Number of Simultaneous Users – The number and distribution of copies must be handled in such way that the number of simultaneous users in a department does not exceed the number of original copies purchased by that department, unless otherwise stipulated in the purchase contract.

Copyrights – In addition to software, all other copyrighted information (text, images, icons, programs, etc.) retrieved from computer or network resources must be used in conformance with applicable copyright and other law. Copied material must be properly attributed. Plagiarism of computer information is prohibited in the same way that plagiarism or any other protected work is prohibited.

Integrity of Information Resources
Computer users must respect the integrity of computer-based information resources.

Modification or Removal of Equipment – Computer users must not attempt to modify or remove computer equipment, software, or peripherals that are owned by others without proper authorization.

Unauthorized Use – Computer users must not interfere with others access and use of the District computers. This includes but is not limited to: the sending of chain letters or excessive messages, wither locally or off-campus; printing excess copies of documents, files, data, or programs, running grossly inefficient programs when efficient alternatives are known by the user to be available; unauthorized modification of system facilities, operating systems, or disk partitions; attempting to crash or tie up a District computer or network; and damaging or vandalizing District computing facilities, equipment, software or computer files.

Unauthorized Programs - Computer users must not intentionally develop or use programs which disrupt other computer users or which access private or restricted portions of the system, or which damage the software or hardware components of the system. Computer users must ensure that they do not use programs or utilities that interfere with other computer users or that modify normally protected or restricted portions of the system or user accounts. The use of any unauthorized or destructive program will result in disciplinary action as provided in this procedure, and may further lead to civil or criminal legal proceedings.

Unauthorized Access
Computer users must not seek to gain unauthorized access to information resources and must not assist any other persons to gain unauthorized access.

Abuse of Computing Privileges – Users of District information resources must not access computers, computer software, computer data or information, or networks without proper authorization, or intentionally enable others to do so, regardless of whether the computer, software, data, information, or network in question is owned by the District. For example, abuse of the networks to which the District belongs or the computers at other sites connected to those networks will be treated as an abuse of District computing privileges.

Reporting Problems – Any defects discovered in system accounting or system security must be reported promptly to the appropriate system administrator so that steps can be taken to investigate and solve the problem.

Password Protection – A computer user who has been authorized to use a password- protected account may be subject to both civil and criminal liability if the user discloses the password or otherwise makes the account available to others without permission of the system administrator.

Usage

Computer users must respect the rights of other computer users. Attempts to circumvent these mechanisms in order to gain unauthorized access to the system or to another person's information are a violation of the District procedure and may violate applicable law.

Unlawful Messages – Users may not use electronic communication facilities to send defamatory, fraudulent, harassing, obscene, threatening, or other messages that violate applicable federal, state or other law or District policy, or which constitute the unauthorized release of confidential information.

Commercial Usage – Electronic communication facilities may not be used to transmit commercial or personal advertisements, solicitations or promotions (see Commercial Use, below). Some public discussion groups have been designated for selling items by IVC OpenComm and may be used appropriately, according to the stated purpose of the group(s).

Information Belonging to Others – Users must not intentionally seek or provide information on, obtain copies of, or modify data files, programs, or passwords belonging to other users, without the permission of those other users.

Rights of Individuals – Users must not release any individual's (student, faculty, or staff) personal information to anyone without proper authorization.

User Identification – Users shall not send communications or messages anonymously or without accurately identifying the originating account or station.

Political, Personal and Commercial Use – The District is a non-profit, tax-exempt organization and, as such, is subject to specific federal, state and local laws regarding sources of income, political activities, use of property and similar matters.

Political Use – District information resources must not be used for partisan political activities where prohibited by federal, state or other applicable laws.

Personal Use – District information resources should not be used for personal activities not related to District functions, except in a purely incidental manner. If the District otherwise grants access to the District's email system for personal use, employees may use the District's email system to engage in protected concerted activity during non-work time.

Commercial Use - District information resources should not be used for commercial purposes. Users also are reminded that the ".cc" and ".edu" domains on the Internet have rules restricting or prohibiting commercial use, and users may not conduct activities not authorized within those domains.

Nondiscrimination

All users have the right to be free from any conduct connected with the use of Imperial Community College District network and computer resources which discriminates against any person on the basis of an ethnic

group identification, gender, gender identity, gender expression, genetic information, pregnancy, race, color, national origin, religion, age, sex, physical disability, mental disability, ancestry, sexual orientation, language, accent, citizenship status, transgender status, parental status, marital status, economic status, veteran status, medical condition, or on the basis of these perceived characteristics, or based on association with a person or group with one or more of these actual or perceived characteristics (See AP 3410).

No user shall use the District network and computer resources to transmit any message, create any communication of any kind, or store information which violates any District procedure regarding discrimination or harassment, or which is defamatory or obscene, or which constitutes the unauthorized release of confidential information.

Disclosure

No Expectation of Privacy – The District reserves the right to monitor all use of the District network and computer to assure compliance with these policies. Users should be aware that they have no expectation of privacy in the use of the District network and computer resources. The District will exercise this right only for legitimate District purposes, including but not limited to ensuring compliance with this procedure and the integrity and security of the system.

Possibility of Disclosure – Users must be aware of the possibility of unintended disclosure of communications.

Retrieval - It is possible for information entered on or transmitted via computer and communications systems to be retrieved, even if a user has deleted such information.

Public Records –The California Public Records Act (Government Code Sections 6250 et seq.) includes computer transmissions in the definition of "public record" and nonexempt communications made on the District network and computer must be disclosed if requested by a member of the public.

Litigation – Computer transmissions and electronically stored information may be discoverable in litigation.

Dissemination and User Acknowledgment

All users shall be provided copies of these procedures and be directed to familiarize themselves with them.

A "pop-up" screen addressing the e-mail portions of these procedures shall be installed on all e-mail systems. The "pop-up" screen shall appear prior to accessing the e-mail network. Users shall sign and date the acknowledgement and waiver included in this procedure stating that they have read and understand this procedure, and will comply with it. This acknowledgement and waiver shall be in the form as follows:

Computer and Network Use Agreement (Sample Language)

I have received and read a copy of the District Computer and Network Use Procedures and this Agreement dated, _____, and recognize and understand the guidelines. I agree to abide by the standards set in the Procedures for the duration of my employment and/or enrollment. I am aware that violations of this Computer and Network Usage Procedure may subject me to disciplinary action, including but not limited to revocation of my network account up to and including prosecution for violation of State and/or Federal law.

Accessibility Policy

Overview

Imperial Valley College (IVC) strives to ensure that people with disabilities have access to the same services and content that are available to people without disabilities, including services and content made available through the use of information technology (IT). IT procured, developed, maintained, and used by the IVC should provide substantially similar functionality, experience, and information access to individuals with disabilities as it provides to others. Examples of IT covered by this policy include IVC-owned technology resources in labs, web sites, software systems, electronic documents, videos, and electronic equipment such as information kiosks, telephones, and digital signs.

Policy

Imperial Valley College (IVC) strives to ensure that IT products developed at, purchased by, or used at the University are accessible to all faculty, students, and staff, including those with disabilities. To reach this aspirational goal, those responsible for making decisions about which products to procure must consider accessibility as one of the criteria for acquisition. This is especially critical for enterprise-level systems and other technologies that affect a large number of students, faculty, and/or staff. To help meet this requirement, bidders will be asked to provide information about the accessibility of their products and accessibility assurances will be included in contracts with vendors.

Backup Policy

Overview

The IVC IT Systems Department maintains systems to hold and retain all essential data for each individual department. This storage area, or File Server and My Docs Server as they are referred to, are used to securely store all data for any given department. Because of these centralized storage arrangements, the IVC IT Department is able to offer secure backup capability ensuring all data will be accessible in the event of a disaster or other event in which the data would be destroyed.

This policy establishes regular backup schedules for our file server and my docs server as it pertains to all this data. With that said, this does not pertain to individual, departmental, or computer lab devices, mobile devices, or other portable storage medium where the data resides locally on the device or medium. The IVC IT Department does not backup for any of these types of devices or storage medium.

Policy

Every effort shall be made by the individual departments and employees at IVC to store sensitive, important, and confidential data on their respective folders. As mentioned above, the IVC IT Department cannot be held liable for issues with data stored elsewhere.

Regular backup schedules are in place within the file server and my docs server to ensure that backups occur at regular intervals and over a time span to provide ample opportunity for the IVC IT Department to recover a file, folder, or group of such. It should be noted that the IVC IT Department **does** require immediate notification in the event a file, folder, or collection of either is found to be missing, corrupt, or otherwise damaged. Waiting to inform the IVC IT Department decreases the probability of successful recovery.

For this document, considering the type of hardware described above, normal backups do not necessarily retain the same meaning as when used in conjunction with other hardware devices. Because of this, the following descriptions are provided, based on the current hardware being used, so as to better understand the overall backup process.

- Backups: These refer to snapshots taken of the file structure and database. These snapshots are essentially pointers to changes occurring within the storage device since the last scheduled snapshot. This greatly reduces the file storage requirements necessary to hold backups while still providing the same or superior level of backup capability found in other devices.

- Replication: This refers to the copying process of all data and associated backups from the primary backup device to the secondary backup device. During a replication, all data and backups are replicated so that a mirror copy is retained for off-site, backup capability should a disaster or other issues occur.

Regularly scheduled backups and replications shall be performed by the IVC IT Department using the following schedule:

- All critical servers backed up daily starting at 10:00 PM with two-week retention.
- Differential backup performed on the File Server and My Docs. Backups performed daily every four hours, starting at 4:00AM, with two-week retention.

Electronic Communications Policy

Overview

Electronic communication is necessary to fulfill multiple roles and activities here at IVC. Because of the varying types of electronic communication, we will focus on those used primarily here at IVC:

- Email
- VoIP
- Digital Signage

Email is the official method of communication at IVC, both for students and employees. Business is conducted every day via email. Since email has both positive and negative connotations, it is imperative that we recognize that the positive aspects greatly outweigh the negative aspects. However, we must also realize that the negative aspects exist and ensure that this method of communication is used effectively, efficiently, and for its' intended purpose.

IVC's VoIP phone system is used to transmit and receive audio/video within the institution to facilitate direct communication amongst employees and departments. It is also used to transmit and receive audio outside the institution to facilitate direct communication with vendors, students, other institutions, and other third-party entities. Because of this capability, we must ensure that it is used for work purposes.

Digital signage is used on campus to convey student activities, important academic dates, campus events, and other information to students, employees, and visitors. Since this is also a visual and auditory communication mechanism, it is also important to ensure it is used for its intended purpose as well.

Policy

Regardless of the type of technology being used, electronic communication is meant to serve the needs of the college by sharing information with students, employees, vendors, other state agencies, campus visitors, and other individuals. Because of the unique capabilities of each system it is important to realize that each type of communication method contains unique issues that must be addressed on a case-by-case basis; however, general rules can be set forth to ensure that any communication method is used wisely and according to its intended purpose.

In general, IVC's electronic communication mechanisms are to be used to share information with students, employees, vendors, other state agencies, campus visitors, and other individuals.

It is also important to note that the true definition of information sharing at IVC is to adequately convey the appropriate knowledge so that the College mission is not hindered but enhanced. This information is always to be distributed under the following assumptions:

Electronic communication from a IVC resource…

- …is always understood to represent an official statement from the institution.
- …shall never be used for the creation or distribution of any information that meets the following criteria:
  - Disruptive
  - Offensive
  - Derogatory
  - Specific comments about race, gender, hair color, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin.
  - Any information that could be used to sabotage institutional progress
  - Any personally identifiable information
- …shall not be used for personal gain
- …shall not be used extensively for personal use
- …shall not be used to distribute malicious or harmful software or information.

Note: IVC_OpenComm is an open, opt-in forum than can be used for personal messages and for personal gain. However, messages are still expected to not be offensive or derogatory.

Emergency Notification Policy

Overview

IVC maintains an emergency notification list on the Regroup system that is used to notify all students and employees who have not chosen to opt 'out.' This system is updated daily from the information collected during registration, to reflect the current student data available so that any notification message will be delivered to the required student and employee list. *We recommend that all users verify their at this URL: https://imperial.regroup.com/signup (Use your IVC email address and password for access)..

Policy

The IVC Emergency Notification List is to be used, at all times, for emergency purposes or purposes deemed necessary by the President or designee only. The notification list is to be used to send messages via text to email addresses and mobile phones, via voice to office phones, personal phones, and mobile devices, and via applications to desktops and office phones.

At no time shall this list be used for normal messaging, notifications, or otherwise standard contact as this would compromise the importance of these messages and may create an environment where students and employees are able to overlook these types of messages because of the frequency with which they could occur.

With that said, tests of this system shall be conducted once a year at minimum to ensure the system is functioning properly. Additional tests may be conducted but are not required; however, more than four tests per semester may be too many to retain the importance of such messages when an actual emergency arises requiring the system to be operational.

Only users defined below shall be able to send emergency notification messages via this system:

- President
- Vice Presidents
- Dean of Student Affairs
- Chief Technology Officer
- Other designee deemed necessary by the President

Equipment Configuration Policy

Overview

This policy has been established to create a standard configuration for all technology resources at IVC. Because of the variances between the types, makes, models, configurations, builds, versions, and brands of technology resources available, it is necessary to standardize all technology resources to make service and maintenance easier and also to help keep costs down.

Policy

All employees shall order and utilize equipment that is serviceable and recommended by the IVC IT Department. Since equipment availability changes over time, especially when referring to technology, a comprehensive list indicating appropriate hardware would be virtually impossible to create. Because of this, any individual or department wishing to purchase technology equipment will first consult the IVC IT Department for current specifications for any given piece of equipment.

This applies to any and all technology equipment including, but not limited to:

- Computers (Servers, Desktop, Laptop, Tablets and Mobile Devices, etc.)
- HDTVs
- Printers, scanners, copiers, fax machines, or all-in-one devices
- Projectors, screens, and SmartBoards
- Security Cameras
- VoIP phones
- Software (Application, Operating System, Network-Based, etc.)
- Other technology equipment not specifically mentioned here

As a rule, the campus has standardized on Windows based computers from Hewitt Packard. The IT department will manage and support these devices as part of the current computer fleet; however, the purchase and refresh of these devices will be the responsibility of the department/divisions, unless approved by the President's Cabinet.

Based on a 'case by case' basis, the IT department will manage and support, on a limited basis, non-Windows devices if there is a valid business reason for their use and approval is gained prior to their purchase.

For more details on procedures required to place an order for technology equipment, please see the Equipment Ordering Procedures included in this document for detailed instructions.

Guest/Visitor Access and Technology Use Policy

Overview

IVC maintains an atmosphere that is open and allows guests and visitors access to resources, as long as such access does not compromise the integrity of the systems or information contained within the campus and does not introduce malicious software or intent to the internal network.

Policy

Guest and visitor access shall be classified into two types as described below:

- Standard – Access granted to internet resources and institutional resources located online.
- Special – Access granted above plus any internal access as requested by an individual with the authority to do so:
    - President, Vice President's, Chief Technology Officer, Chief Human Resources Officer, or other designee deemed necessary by the President

Internal Access may include:

- Wireless VLANs (i.e. IVC-Employee, IVC-Student)
- Wired VLANs
- Singular or multiple file access
- System access such as Banner, Canvas, Starfish, etc.

Under no circumstances should visitors be given special access unless permission has been obtained from the appropriate administrative personnel (i.e. a signature from one of the personnel above) along with detailed description of access.

To obtain guest/visitor access users should contact the IVC IT Department with their requested system access requirements using the attached Authorization of User Access form.

For vendor access, please see the appropriate vendor access policy included herein.

Computer Refresh Policy

Overview

Keeping computers and other IT hardware on a predictable replacement cycle is part of the Strategic Technology Plan. It is also beneficial to the efficient function of the campus in many ways. From a general college perspective by replacing the computers on a consistent refresh cycle it helps faculty and staff to be more productive in their day to day work. From an IT perspective it is essential to the tech support philosophy, and staffing decision are built around a consistent refresh cycle. Computers that are replaced on a consistent refresh cycle require less care and maintenance, which in-turn allows us to maintain fewer technicians so that we can move those resources to other areas of need.

To provide for administrative oversight and fiscal planning for any new computer(s) or other devices that a department/division wishes to purchase and add to the computer refresh program, the department/division must first get approval from Cabinet. They will need to fill out the computer request form and get approval signatures from their Dean and/or VP. The request will then go to Cabinet for discussion and approval/denial. If department/division is going to pay for future refresh from their department/division funds, then it does not need to go Cabinet.

The policy is applicable to all computer devices, i.e. laptops, desktops, tablets.

Policy

The goal of the refresh program is to replace the below noted computers on campus over a five (5) year cycle:

- Each staff and faculty member shall be provided a primary desktop computer that will be included in the refresh program to be replaced every 5 years.
- Computers in each of the existing campus labs campus will be replaced on a five (5) year cycle.
    - Existing labs: Math Lab (2500), Reading/Writing Lab (2602), English Lab, 801 Lab, 803 Lab, 901 Lab, 2724 Lab, 3102 Lab, Business Lab(2608), Laptop Carts on Wheels (COWS) in 2700 building, Library ????
- IT department will provide faculty and staff members with a standard commercial quality computer that is expected to remain productive for 5 years.
- In those few circumstances that a standard computer isn't felt to be sufficient to meet the needs of the faculty/staff member. IT will work with the division/department to determine the proper computer for the particular need. However, the final decision is with the IT department.
- If the department/division still wants a computer that exceeds the recommended computer, the department/division will pay for the difference in cost between what is recommended and what they want.
- If a division/department wishes to provide their faculty/staff with a device other than the provided desktop they become responsible for the purchase and refresh of that device, unless approved by Cabinet to be added to the refresh (see refresh request form).
- If a division/department wishes to create a new lab they will be responsible for the purchase.
- Categorical Programs are responsible for paying for the refresh of the computers within their program.
    - IT will let them know a year in advance for budgeting purposes.
    - IT will handle the purchase and installation of the computer.

    - Must be an acceptable expense within their program.
- All computer device purchases have to follow the computer purchasing policy.

Password Policy

(pending re-evaluation of policy taking into consideration recommendation(s) from Security Audit Report)

Password Policy

Password Policy

Personally Identifiable Information Policy

Overview

This policy will establish IVC's definition of Personally Identifiable Information (PII) and indicate what information may be shared, if any, with third-party entities.

Policy

It is important to note that information should never be shared without cause or requirement, unless dictated by state or federal government regulations such as annual reporting guidelines and statistical reporting data, in the course of preset institutional operations or vendor agreements, or due to the request of IVC's President or designee.

PII is the type of information that should be kept safe using the highest level of security. PII is described as information about an individual that identifies, links, relates, or is unique to, or describes him or her. This information may include:

- Name
- SSN
- Address(es)
- Phone Number(s)
- Birth date
- Birth place
- Mother's maiden name
- Family names
- Other family data such as addresses, contact information, etc.
- Financial information such as bank account information, account balances, etc.
- Other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have a personal knowledge of the relevant circumstances, to identify the student with a reasonable certainty
- Information requested by a person who the educational agency or institution believes knows the identity of the student to whom the educational record directly relates

Under no circumstances should PII be transported off-campus. On-campus storage of PII should meet other policy requirements as dictated herein. Off-campus use of this type of data may be facilitated via the IVC IT Department's Remote Access Policy.

Remote Access Policy for Staff

Overview

This policy establishes the official rules set forth to allow users to remotely access and manipulate personally identifiable information, network applications, and other data from off-campus.

Policy

Any user who seeks to work off-campus for the purpose of working from home or at another location can facilitate this through the use of the IVC VPN connection. All users needing access to Banner or other applications requiring network connectivity to the campus can facilitate this by connecting from home via a VPN connection.

This type of connection establishes a secure, encrypted connection, to the campus network to allow the user to manipulate and access the data at a distance. At no time should any PII be transferred off-campus on any type of device. If a given user wishes to work while off-campus, he/she should use the enclosed Remote Access Procedure to obtain a secure connection to the network and work from a distance.

This type of connection allows the user to remotely manipulate and access the data without actually transferring any data off-site thus ensuring all PII and other data is kept safe and secure from unauthorized access.

Remote access will only be set up on IVC owned and issued equipment. A security certification will be installed on the device to validate the connection and secure the transfer of data.

Vendor Access Policy

Overview

This policy will set forth parameters for vendors to abide by when access to our internal or external network, workstations, or servers is required. All vendors, regardless of status, frequency of visitation, work being performed, or size of entity shall abide by this policy at all times unless such work does not require access to the IVC network or computing resources.

Policy

All vendors shall notify their contact on campus of any work that will require access to any of the following IVC resources:

- Internal network
- External network
- On-campus workstation(s)
- On-campus server(s)
- Network infrastructure
- Any other computing device on campus

Upon notification of the need for access, the IVC IT Department shall create login credentials and access requirements necessary to facilitate the access required for the vendor to complete their job function. Access shall always be restrictive meaning un-warranted or un-needed access will not be available until deemed necessary by the requirements of the project. All requests for access shall be evaluated on a case-by-case basis to ensure that proper access is granted and no un-warranted or un-needed access is given without cause.

At all times, the vendor shall…

- Fulfill their primary job responsibility only;
- Not seek to undermine or circumnavigate the access which has been provided;
- Not tamper or adjust security settings on existing network infrastructure or devices;
- Ensure that access credentials are not shared with anyone other than those individual approved for access;
- Work to ensure that IVC's information is kept safe and secure from loss or theft;
- Never disclose any information he or she may come to know from working with or on any IVC technology resource with a separate third-part entity;
- Notify the IVC IT Department IMMEDIATELY upon any inclination that loss or theft has occurred, access has been lost or tampered with, or there is a concern that any other type of access violation has occurred;
- Never seek to use any of IVC's information for personal or other monetary gain;
- Not use any access or technology resource in a manner that has been prohibited for employees, students, or visitors in any of the other, enclosed policies herein.

Procedure

If any vendor requires access to technology resources, please follow these steps:

1. Submit Authorization of User Access Form to IVC IT Department.
2. IT Department will evaluate request and grant access based upon need and policies.
3. Vendor access will be created to comply with existing policies.
4. Requesting employee will receive email once appropriate access has been created.

Procedures

Equipment Ordering Procedure (Angie is updating)

This document is to serve as a set of guidelines for all IVC Faculty and Staff who choose to order computing equipment.

1. Either contact the IVC IT Department to obtain the project request form or down load it from the IVC web page at Equipment Request Form.
2. Once form is completed please send to itprojectrequests@imperial.edu
3. Form will be taken to Cabinet for approval.
4. IT Department will request the quote(s) from the vendors.
5. Quotes will be forwarded to you for approval.
6. Once approved IT will submit your order.
7. Once your order has been placed, you may check on the progress by contacting the IT department
8. When your equipment arrives, the purchasing should deliver the equipment to the IT Department. Once the IT Department has received the equipment and configure it, if necessary, it will be delivered or installed as necessary.
   NOTE: All technology orders must be received by the IT Department before it can be released to the purchaser. This is to ensure that the proper software is installed and all equipment is properly tagged and placed in inventory.

Remote/VPN Access Procedure

For users that require access to sensitive information at home or on the road, access procedures will be provided AFTER request has been approved by the Chief Technology Officer.

Terms and Definitions

Appropriate Measures

Refers to the measures that the IVC IT Department is authorized to take to secure IVC's computing resources. This may refer to measures concerning IVC owned hardware or software, data, employees, students, associates, visitors, etc. The IVC IT Department must maintain an appropriate measures option so that IVC is protected, concerning both equipment and information.

Approved Electronic File Transmission Methods

Includes supported FTP clients including, but not limited to, FileZilla, SecureFTP, and SmartFTP. This also includes supported Web browsers including, but not limited to, Microsoft Internet Explorer, Mozilla Firefox, Netscape Navigator, and Opera. If you have a business need to use other mailers contact the IVC IT Department prior to implementation.

Approved Electronic Mail

Includes all mail systems supported by the IVC IT Department. This includes, but is not limited to, IVC Webmail, Outlook configured email, and configured email on mobile devices. If you have a business need to use other mailers contact the IVC IT Department prior to implementation.

Approved Encrypted Email and Files

Techniques include the use of AES and others. Please contact the IVC IT Department for further information.

Asymmetric Cryptosystem

A method of encryption in which two different keys are used: one for encrypting and one for decrypting the data (e.g., public-key encryption).

Chain email or letter

An email sent to successive people. Typically, the body of the note has direction to send out multiple copies of the note and promises good luck and/or money if the directions are followed.

Information System Resources

Information System Resources include, but are not limited to, all computers, peripherals, data, and programs residing on the IVC Campuses, networks, servers, etc. These resources also include all paper information and any information for internal use only and above.

Information Technology Systems

The technology department responsible for managing IVC's computing resources.

Configuration of IVC-to-Third Party Connections

Connections shall be set up to allow third parties requiring access to the IVC campuses, networks, data, etc. These connections will be setup in order to allow minimum access so that third-party

entities will only see what they need to see, nothing more. This involves setting up access, applications, and network configurations to allow access to only what is necessary.

Domain Name System

Essentially serves as the Internet “phone book” by associating various domain names (i.e. http://www.connorsstate.edu, http://it.connorsstate.edu) with their counterpart IP addresses that the computers and networking equipment need to transmit data.

Email

The electronic transmission of information through a mail protocol such as SMTP, IMAP, or Exchange. Typical email clients include Mozilla Thunderbird and Microsoft Outlook.

Encryption

This refers to the modification and storage of data by manipulating the way it is stored through the use of an algorithm. An encryption key is required to gain access to the original data and therefore provides the security desired.

Encryption Key

A software key used to gain access to encrypted data.

Expunge

To reliably erase or remove data on a PC or Mac you must use a separate program to overwrite data. Otherwise, the PC or Mac's normal erasure routine keeps the data intact until overwritten which may allow the PC to actually retain the “deleted” information for some time after the deletion took place.

Forwarded email

Email received from one sender and then sent to another recipient.

Individual Access Controls

Methods of electronically protecting files from being accessed by people other than those specifically designated by the owner. This includes the utilization of passwords, screensavers, hardware encryption, etc.

Insecure Internet Links

All network links that originate from a locale or travel over lines that are not totally under the control of IVC. These types of connections can allow an unidentified third-party to intercept, monitor, or copy the traffic being sent across this connection.

Internet

A worldwide, publicly-accessible series of interconnected networks used to transmit packets of data via the Internet Protocol (IP).

Internet Protocol

A data-oriented network protocol used to transmit data across a packet-switched network such as the Internet.

Local Area Network

A computer network covering a small geographic area. These can include a single campus, a single building, or even a single room.

One Time Password Authentication

This type of authentication is accomplished by using a one-time password token to connect to a network resource or reset a network account. As long as the connection remains open the password token is retained and access is allowed.

OSU A&M System

The system of collaborative institutions including Connors State College, Langston University, Northeastern Oklahoma Agricultural and Mechanical College, Oklahoma Panhandle State University, Oklahoma State Center for Health Sciences, Oklahoma State University – Okmulgee, Oklahoma State University – Oklahoma City, Oklahoma State University – Tulsa, Oklahoma State University – Stillwater, Oklahoma State University – Center for Veterinary Health Sciences, Agricultural Experiment Station, and Cooperative Extension Service.

Personal Computer

A device used by a single user to access local programs and files, network resources, or the Internet. This can include desktop, laptop, tablet, or portable computers.

Physical Security

Physical security refers to the actual physical security mechanisms in place to prevent unauthorized access to technology resources. This can also mean having actual possession of a computer or by locking the computer in an unusable state to an object that is immovable. Methods of accomplishing this include having a special key to unlock the computer so it can be used, thereby ensuring that the computer cannot be simply rebooted to get around the protection. If it is a laptop or other portable computer, never leave it alone in a conference room, hotel room, in a vehicle, on an airplane seat, etc. Make arrangements to lock the device in a secure location such as a hotel safe or take it with you. In the office, always use a lockdown cable. When leaving the office for the day, secure the laptop and any other sensitive material in a locked drawer, cabinet, safe, etc. or simply take it with you.

Private Link

An electronic communications path for which IVC has control over the entire distance. These types of links typically use a VPN tunnel or other means to connect two or more locations. For example, all IVC networks are connected via a private link. IVC also maintains private links to OSU and other A&M institutions.

Proprietary Encryption

An algorithm that has not been made public and/or has not withstood public scrutiny. The developer of the algorithm could be a vendor, an individual, or the government.

Public Link

An electronic communications path for which IVC does not have control over the entire distance. This connection does not utilize any special connection scheme. A connection from any IVC computer to the Internet is an example of a public link.

Secure Internet Links

All network links that originate from a locale or travel over lines that are either under the control of IVC or utilize technology to form a secure “pipe” for information to traverse. These types of connections prohibit an unidentified third-party to intercept, monitor, or copy the traffic being sent across this connection by solely utilizing the IVC network or utilizing a secure authentication mechanism to connect

Sensitive information

Information is considered sensitive if it can be damaging to IVC, its employees, students, associates, etc. This information can include personnel data, student information, purchasing information, etc.

Symmetric Cryptosystem

A method of encryption in which the same key is used for both encryption and decryption of the data.

Unauthorized Disclosure

The intentional or unintentional revealing of restricted information to individuals, either internal or external to IVC, who do not have a need to know that information.

User Authentication (Local)

A method by which the user of a system can be verified as a legitimate user on that system only.

User Authentication (Network)

A method by which the user on a network can be verified as a legitimate user independent of the computer or operating system being used.

Virtual Private Network

A network that functions as a single, secure network that is usually comprised of several locations residing in separate geographic areas. This is accomplished through the use of secure, authenticated connections from one network to another.

Virus Warning

Typically, these are emails containing warnings about virus or mal-ware. The overwhelming majority of these emails turn out to be a hoax and contain bogus information usually intent only on frightening or misleading users. However, the IVC IT Department occasionally sends out virus warning should the need arise. In these cases, recipients should heed the warnings provided by the IT Department employees rather than treat the information as potentially misleading.

Wide Area Network

A computer network covering a large geographic area. The Internet is an example of a WAN.

Disclaimer

The IVC IT Department regards this document as a work in progress. Because of this, these policies and procedures undergo regular reviews and modifications. Therefore, it is up to each individual employee or associate to remain current on the updated policies and procedures.

Changes in these policies and procedures after the initial agreement signature date does not allow non-compliance or permit the employee or associate to engage in activities contradictory to the modifications made after the initial agreement signature date.

Forms

Authorization of User Access Form

User requesting access: _____

Name: _____ CWID: _____

Email Address: _____

Cell Phone: _____

Employee making request: _____

Name: _____

Email Address: _____

Title: _____

Type of access needed: _____

System: _____ Duration: _____

System: _____ Duration: _____

System: _____ Duration: _____

System: _____ Duration: _____

System: _____ Duration: _____

Special Requirements: _____

_____

_____

_____

IVC IT Department Personnel Use Only: _____

Receiving Employee: _____ Date: _____

Access Created? Yes – No – Other: _____ Date: _____

Details: _____

Equipment Transfer Form

User receiving equipment: _____

Name: _____ Company: _____

Email Address: _____

Cell Phone: _____

Employee transferring equipment: _____

Name: _____ Date: _____

Email Address: _____

Title: _____

Equipment being transferred: _____

Item 1: _____ Serial #: _____ IVC #: _____

Item 2: _____ Serial #: _____ IVC #: _____

Item 3: _____ Serial #: _____ IVC #: _____

Item 4: _____ Serial #: _____ IVC #: _____

Item 5: _____ Serial #: _____ IVC #: _____

Item 6: _____ Serial #: _____ IVC #: _____

Item 7: _____ Serial #: _____ IVC #: _____

Item 8: _____ Serial #: _____ IVC #: _____

Item 9: _____ Serial #: _____ IVC #: _____

Item 10: _____ Serial #: _____ IVC #: _____

Special Requirements/Notes: _____

_____

IVC IT Department Personnel Use Only: _____

Receiving Employee: _____ Date Received: _____

Details: _____