Computer Security and Policy

Education and Training for IT Service Providers at UCSC

2015-2016
Training Requirements

- All new ITS employees must complete this training within **one month** of their start date and provide the certificate of completion to their supervisor.

- Continuing ITS employees must complete training refreshers as announced, approximately annually.

- Additional required training based on access:
  - HIPAA training for ITS staff with access to HIPAA data or systems: [http://its.ucsc.edu/security/training/hipaa.html](http://its.ucsc.edu/security/training/hipaa.html)
  - PCI training for ITS staff with access to credit card data or systems: [http://its.ucsc.edu/security/training/its-staff.html](http://its.ucsc.edu/security/training/its-staff.html)

- Training requirements are also included in ITS’ onboarding checklist: [http://its.ucsc.edu/internal/supervisor-resource.html#onboard](http://its.ucsc.edu/internal/supervisor-resource.html#onboard)
Topics

- IT Service Provider Responsibilities
- Access Principles
- Sensitive Data: Definitions and Protection
- Key Security Practices for IT Service Providers
- Acceptable Use and Personal Use
- Reporting Security Incidents
- Additional Resources;
  Appendices: List of Links and List of Contacts
- Test Your Understanding
Topics

- **IT Service Provider Responsibilities**
- Access Principles
- Sensitive Data: Definitions and Protection
- Key Security Practices for IT Service Providers
- Acceptable Use and Personal Use
- Reporting Security Incidents
- Additional Resources; Appendices: List of Links and List of Contacts
- Test Your Understanding
IT professionals and people with privileged access have a level of responsibility above and beyond what other people have.
Some Specific Responsibilities (1 of 3)

- Keep systems up and running so the University can do its business
- Understand and comply with UC and UCSC IT policies, procedures, and guidelines, relevant laws and industry requirements, and provide this information to clients as appropriate
- Implement appropriate security measures - in coordination with the System Steward/business partner, where applicable
  - This includes routinely evaluating resources against potential and known threats
- Help clients protect information properly and understand their responsibility for doing so
Some Specific Responsibilities (2 of 3)

- Assess and advise System Stewards/business partners on risks, threats, options and tradeoffs so they can make informed risk tolerance/acceptance decisions

  - Implicit in this is that ITS staff are not to make business-related risk decisions on behalf of non-ITS partners. ITS’ role in this case is typically to advise System Stewards/business partners so they can make informed risk decisions.

  - This is not intended to imply that ITS staff must consult non-ITS partners for risk decisions entirely within ITS’ purview. For example, ITS has the independent authority to make risk decisions and follow procedures for blocking network access and compromised accounts to address threats that may pose a serious risk to campus information system resources. See Procedures for Blocking Network Access: http://its.ucsc.edu/policies/blockingproc.html.
Some Specific Responsibilities (3 of 3)

- Respond to potential security breaches according to campus incident response procedures (additional info later in this training)

- Use appropriate professional practices in providing for the security of the systems and data you use or manage
  - This includes appropriate separation of duties and change management
Requirements Associated with Privileged Access (1 of 2)

Definition: Privileged access is any access to systems, applications, databases, etc. that enables a user to carry out system administration functions, or that provides broad access to personal or institutional information.

Use of Privileged Access:
- Privileged accounts are only to be used for authorized purposes.
- Individuals must receive appropriate authorization and training before making use of privileged access – even if the account is all set up and ready to go.
- Every account holder is responsible for understanding about appropriate access and disclosure of information. An overview is included in this training.

Review of Privileged Access:
- Activities performed using privileged accounts should be logged – either by the system/application or manually. These logs should be reviewed on a regular basis by the responsible sys/app admin to ensure appropriate use.
Management of Privileged Access:

- Privileged access will be removed or modified as appropriate when account holders leave their job or change job duties.
- Privileged access will normally be revoked or modified for individuals on investigatory leave or under disciplinary action.
- The number of privileged accounts should be kept to a minimum, and only provided to personnel whose job duties require them.
- People who require privileged accounts should also have non-privileged accounts to use when not performing system administration tasks and should be instructed not to use their privileged accounts for non-authorized purposes.
- ITS staff members will be background checked upon hire or job change.
Topics

- IT Service Provider Responsibilities
- **Access Principles**
- Sensitive Data: Definitions and Protection
- Key Security Practices for IT Service Providers
- Acceptable Use and Personal Use
- Reporting Security Incidents
- Additional Resources; Appendices: List of Links and List of Contacts
- Test Your Understanding
Food for Thought (1 of 2)

Consider the proper thing to do in the following situations (answers later)

1. You ask your assistant to make an office birthday calendar. He uses his Payroll/Personnel System (PPS) access to look up everyone’s birthday for the calendar.

2. The Support Center and abuse@ucsc.edu get a report that a student is posting negative comments about a member of the UCSC community on the student’s personal UCSC web page. The person making the report wants the web page removed and the student disciplined.

3. The Support Center gets a ticket explaining that a highly sensitive, personal email was accidentally sent to the wrong person. The request is for ITS to find and delete the email.

4. You get a call from the Title IX/Sexual Harassment Office. They need the IP address associated with a specific harassing email. They have a copy of the email.
Food for Thought (2 of 2)

Consider the proper thing to do in the following situations (answers later)

5. A lawyer contacts one of our network techs to ask whether netflow logs are available for a specific date range. The lawyer isn’t asking for the information, she is just asking if we have it to determine if it is worth the time to get a subpoena.

6. A Desktop Support tech is working on a computer and sees some really great music he would like to have.

7. Networking discovers a machine that is sending a huge amount of data through our network. They have determined that the pattern looks like P2P filesharing activity. This could mean illegal filesharing or maybe a compromised machine. The person on duty is contemplating looking at what is being sent (the actual content of the files) to see if he can tell what is going on.

8. A Local IT Specialist (LITS) needs to wipe the hard drive of a former employee’s computer so the division can re-assign it to another employee. He is wondering if he needs the ex-employee’s permission or some other authorization to access the computer.
Access Principles

Most ITS employees have broader access to systems and data than they have an actual business need for.

- You are responsible for only using your access for the purposes for which it was provided
  - Just because you can do something, just because you can look at something, just because “everyone does it”, doesn’t necessarily mean it’s OK to do so.

- Don’t share confidential or restricted information with people who don’t have a business need to know it or aren’t authorized for the information
  - This includes information you may incidentally observe in the regular course of your duties
What About Routine Monitoring?

*Routine monitoring* is the term UC uses to describe the regular monitoring of systems and networks “to ensure their integrity, reliability and security”.

Employees who perform routine monitoring must not inspect or peruse the actual contents of what they are monitoring beyond what is necessary to accomplish this task. They also must not seek out content unless it is directly related to the monitoring.

If, during the course of your regular duties, you happen to observe a violation of law or policy that must be reported, report it to the appropriate office or authority. Do not, however, examine the content beyond what is necessary for your job duties. See the following slides on accessing electronic communications records for additional information.

**Additional information:**
- Routine monitoring practices at UCSC: [http://its.ucsc.edu/policies/monitoring.html](http://its.ucsc.edu/policies/monitoring.html)
- UC policy for routine monitoring activities: The UC Electronic Communications Policy (UC ECP), Sec IV.C 2.b and V.B: [http://policy.ucop.edu/doc/7000470](http://policy.ucop.edu/doc/7000470)
What About Accessing Electronic Communications Records? (1 of 4)

Definition: Electronic communications records are any information that has been transmitted electronically. This includes files, email and email attachments, and information from transactional logs. It also includes any combination of these that may provide details about an individual’s activities.

UC policy says that except under specific circumstances, permission is needed to access an individual’s electronic communications records, even after the person has separated from the University. The next two slides describe when permission is and is not needed.

If you are ever in doubt about whether you are allowed to access, release or disclose electronic communications records, contact the IT policy office, Janine Roeth and Julie Goldstein, at itpolicy@ucsc.edu or 9-2779.
What About Accessing Electronic Communications Records? (2 of 4)

Permission or authorization is required for you to:

- Release or disclose information that is not publicly available
- Provide anyone access to another person’s electronic communications records, including their files or email, even if the person has left the University or is deceased
- Examine the actual contents of other people’s computers, files, emails, telephone conversations, etc.
- Seek out or disclose information relating to an individual’s activities
- Examine the contents of electronic communications beyond what you must observe to carry out your regularly assigned job duties

As a general rule, ask the owner(s) or holder(s) of the information (the “record holder”) for permission. If this isn't possible or practical, such as in the case of an investigation or if the person is not available, UCSC’s formal “access without consent” process must be followed, regardless of who is requesting the information.

- The process and authorization form are available online at http://its.ucsc.edu/policies/docs/ecpform.pdf
What About Accessing Electronic Communications Records? (3 of 4)

Special permission or authorization is not required for you to:

- Release or disclose information that is publicly available
- Help someone understand information in their possession
- Carry out your regularly assigned job duties. This includes routine monitoring (see slide 15).

**Clarification about working on people’s systems/accounts:**
As long as it’s consistent with your job duties, you are allowed to work on people’s systems or accounts even when there might be incidental exposure to actual content. You may not, however, seek out or examine specific individuals’ email, files, content, etc. without special permission or authorization. You also must not disclose specific content you may have incidentally observed.
What About Accessing Electronic Communications Records? (4 of 4)

Overarching Principles to Remember:

- “Least perusal”: Always access the minimum amount of other people’s content or information possible in order to perform your job duties.
- Don’t seek out information beyond the scope of your defined job duties. This includes information about individual users’ activities or the contents of their electronic communications.
- Only use your access for the purposes for which it was authorized.
- Don’t release or disclose information to people who aren’t authorized to have it.

If you have been asked or think you need to access or investigate records beyond the threshold of your defined job duties, or if you aren’t sure whether authorization is required, **STOP**. Get permission from the record holder, or contact the IT policy office for instructions: itpolicy@ucsc.edu or 9-2779.
A Special Note about Access to Employee Records upon Separation

Information about access to and disposition of employee records upon separation is available at http://its.ucsc.edu/policies/access-notice.html

Where units/departments incorporate this notice or an equivalent into their on and offboarding processes, it is not necessary for them to obtain special permission to access a separated employee’s records in the case of normal (voluntary, non-volatile) separations. Otherwise, the unit needs to obtain the ex-employee’s permission or get special authorization for access, as mentioned on the previous slides.

ITS has incorporated information from this notice, as well as other related procedures, into our onboarding and offboarding checklists. Supervisors are expected to follow these checklists, available at http://its.ucsc.edu/internal/supervisor-resource.html#onboard

To avoid business continuity issues, supervisors should ensure departing employees transfer ownership of all University records, including email and Docs, to their successor, supervisor, or other identified individual(s) before leaving.
What About Requests for Information?

- Requests for information from the FBI or other federal agents: All communication must go through Campus Counsel: 459-1848 or campuscounsel@ucsc.edu. **Do not** provide any information to the agent directly, including information about what we would be able to produce were they to obtain a warrant or subpoena.

- Requests for information that is available to the public: If the information is available to the public you may provide it. Or if the requester is already in possession of the information and just needs assistance understanding or accessing it, you can help them.

- Refer other requests for information to the IT policy office: Janine Roeth and Julie Goldstein - itpolicy@ucsc.edu

- All of the above apply even if an “authoritative” person is asking, like the Police or the Title IX/Sexual Harassment Office.
What About Complaints About Harassment, Safety or Improper Activity?

- In general, we (ITS) should not attempt to evaluate or respond to improper activity complaints that fall outside of ITS’ purview. If you receive complaints about harassment or life/safety concerns, report them to expert partners like the Campus Police, Title IX/ Sexual Harassment. Don’t launch an investigation on your own beyond what would be normal in the course of your job.

- We’ve been encouraged to refer other complaints of improper or potentially illegal activity to the Whistleblower Policy Office: http://whistleblower.ucsc.edu/

- If you’re not sure who to contact, contact the IT policy office for assistance: itpolicy@ucsc.edu
Restricting Someone’s Access (1 of 2)

- Service Providers are allowed to wholly or partially restrict services or resources in order to control an emergency or prevent damage or loss. This authority also permits disabling account credentials that are reasonably believed to be compromised.

- ITS has specific procedures for blocking network access and responding to accounts/passwords that show evidence of compromise: http://its.ucsc.edu/policies/blockingproc.html and IT Request tech-only Knowledge Base (KB) article #16640.

- UCSC’s Electronic Communications Policy (Sec. VII.1) addresses authority for copyright notice response: http://policy.ucop.edu/doc/7000470
Restricting Someone’s Access (2 of 2)

- For situations other than those described on the previous page, authorization at the following level is generally required to restrict someone’s access to electronic communications services or resources:
  - CP/EVC for students
  - Unit/Department Head or Dean for staff and academic employees
  - VC BAS for non-university individuals

Please contact the IT policy office for assistance with the approval process: itpolicy@ucsc.edu
Food for Thought – The Answers

1. **Situation:** You ask your assistant to make an office birthday calendar. He uses his PPS access to look up everyone’s birthdays for the calendar.

   **What to do:** The assistant should have asked the employees for their birthdays. It’s not OK to use access for something other than the purpose for which it was granted, and chances are his PPS access is not for the purpose of looking up people’s birthdays for an office calendar. As a supervisor, you should consider whether a formal reprimand, counseling memo, or other action may be in order.

2. **Situation:** The Support Center and abuse@ucsc.edu get a report that a student is posting negative comments about a member of the UCSC community on the student’s personal UCSC web page. The person making the report wants the web page removed and the student disciplined.

   **What to do:** Is this a policy violation or freedom of speech? Refer this person to the Whistleblower Office. They will determine whether there are any law or policy violations, and what to do, if anything. Also send a copy of the ticket to the Whistleblower Office.
3. **Situation:** The Support Center gets a ticket explaining that a highly sensitive, personal email was accidentally sent to the wrong person. The request is for ITS to find and delete the email.

**What to do:** The Support Center may not delete - or even access - someone’s electronic communications without their permission. The requester would either need to get the recipient’s permission or go through the “access without consent” process.

4. **Situation:** You get a call from the Title IX/Sexual Harassment Office. They need the IP address associated with a specific harassing email. They have a copy of the email.

**What to do:** If the email still has the full headers, you can help the Title IX folks obtain the IP address from the headers. This is because the Title IX Office already possesses the information; you’re just helping them access it. If the email doesn’t have the headers anymore, it’s not OK to go fishing around to try to find an intact copy of the email without obtaining special permission to do so. The Title IX Office would need to initiate the process of obtaining permission.
Food for Thought – The Answers

5. **Situation:** A lawyer contacts one of our network techs to ask whether netflow logs are available for a specific date range. The lawyer isn’t asking for the information, she is just asking if we have it to determine if it is worth the time to get a subpoena.

**What to do:** Do not provide this information. Explain to the person that this type of request needs to go to the IT policy office (Janine Roeth or Julie Goldstein). The person could also be referred directly Campus Counsel’s office. Feel free to provide direct contact information: 459-1848 or campuscounsel@ucsc.edu

6. **Situation:** A Desktop Support tech is working on a computer and sees some really great music he would like to have.

**What to do:** Stop looking around at the contents of the customer’s computer. Definitely don’t copy the music; purchase it legitimately.
7. **Situation:** Networking discovers a machine that is sending a huge amount of data through our network. They have determined that the pattern looks like P2P filesharing activity. This could mean illegal filesharing or maybe a compromised machine. The person on duty is contemplating looking at what is being sent (the actual content of the files) to see if he can tell what is going on.

**What to do:** Inspecting the actual content of someone’s transmissions (beyond incidental exposure while carrying out routine job duties) requires special permission or authorization. Just notify the usual contacts about the activity and that it looks like P2P. If there were a legitimate need to inspect the actual contents of the traffic, the tech would need to get the individual’s permission or go through the “access without consent” process (and justify the need to do so).

8. **Situation:** A Local IT Specialist (LITS) needs to wipe the hard drive of a former employee’s computer so the division can re-assign it to another employee. She is wondering if she can do this without the ex-employee’s permission.

**What to do:** The LITS can go ahead and wipe the drive, but may not inspect drive contents.
Access to Information Statement

The *University Administrative Information System Access to Information Statement* addresses appropriate access and disclosure of electronic information at UCSC: [http://its.ucsc.edu/accounts/docs/access-info-stmt.pdf](http://its.ucsc.edu/accounts/docs/access-info-stmt.pdf)

Because most ITS employees have access to a wide range of protected, often personal information, all ITS employees, including student employees, must read and sign the *Access to Information Statement*.

- Send signed Statements to the Accounts Team in the ITS Support Center (mailstop: ITS-Kerr).

- **Note:** You only need to read and sign the *Access to Information Statement* once. If you have *not* already completed it (or can’t remember), you can download it from the above link.
Topics

- IT Service Provider Responsibilities
- Access Principles
- **Sensitive Data: Definitions and Protection**
- Key Security Practices for IT Service Providers
- Acceptable Use and Personal Use
- Reporting Security Incidents
- Additional Resources;
  Appendices: List of Links and List of Contacts
- Test Your Understanding
Levels of Sensitivity

Confidential Information:
The term “confidential information” applies broadly to information for which unauthorized access or disclosure could result in an adverse effect. To address this risk, some degree of protection or access restriction may be warranted.

Restricted Data:
Restricted data is the most sensitive confidential information. Restricted data is any confidential or personal information that is protected by law or policy and that requires the highest level of access control and security protection, whether in storage or in transit.
Examples of Restricted Data

- Personal Identity Information (PII) - see slides 35-37
- Credit card data regulated by the Payment Card Industry (PCI) - see slide 38
- Electronic protected health information (ePHI) protected by Federal HIPAA legislation - see slides 39-40
- Passwords providing access to restricted data or resources
- Information relating to an ongoing criminal investigation
- Court-ordered settlement agreements requiring non-disclosure
- Information specifically identified by a unit or department, or by contract, as restricted.
Examples of Non-Restricted Confidential Information

- Home address or home telephone number
- Personal information protected by anti-discrimination and information privacy laws, such as
  - ethnicity or gender
  - date of birth
  - citizenship
  - marital status
  - religion or sexual orientation
- Certain types of student records (see slides 41-42)
- Exams, answer keys, and grade books
- Applicant information in a pending recruitment
More Examples of Non-Restricted Confidential Information

- Security information that may allow an attacker access to IT resources
- Information subject to a non-disclosure agreement, including research data, intellectual property (IP), and patent information, and other proprietary data
- Academic evaluations and letters of recommendation
- Responses to a Request for Proposal (RFP) before a decision has been reached
- Certain kinds of personnel actions
- “Pre-decisional” budget projections for a campus department (can also be marked “Draft” or “Not for Distribution”)
Definitions of Selected Types of Restricted Data (1 of 8)

Personal Identity Information (PII):

PII is the electronic manifestation of an individual’s first name or first initial, and last name, in combination with one or more of the following*:

- Social Security Number (SSN)
- Driver’s license number or State-Issued ID card number
- Financial account, credit card, or debit card number
- Medical information – the definition of medical PII is broader than HIPAA
- Health insurance information – ditto

We need to protect PII in order to protect people from potential identity theft. State law also requires us to notify people if there is a reasonable belief that their PII has been accessed without authorization. This puts PII in a high priority category for requiring protection.

* Please note, this is a condensed list. For a more complete definition please see ITS’ online glossary: http://its.ucsc.edu/policies/glossary.html#pii
Checking for PII

ITS staff are responsible for initiating checks of systems for PII in response to the following triggers.

- Re-purposing/re-assigning a computer
- Transferring files from an old computer to a replacement computer
- Response to a potential security breach
- DL/Local IT Specialist acquiring a new server to support or manage
- New server going into the ITS Data Center
- Development or acquisition of a new application
- Equipment or media disposal
- When an individual changes jobs and takes their files with them

PII checks must be done in coordination with the data/system owner, and the access principles in the previous section of this training must be followed. **PII should be removed when possible and properly protected if removal is not possible.**

→ ITS’ PII scanning methodology: [http://its.ucsc.edu/policies/ssnscan.html](http://its.ucsc.edu/policies/ssnscan.html)
More on PII:

PII is Protected by Law and UC Policy

- **State Law:** California Civil Code 1798.29 requires us to notify people if their unencrypted PII is disclosed without authorization.
  
  http://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=CIV&division=3.&title=1.8.&part=4.&chapter=1.&article=7

- **UCSC Policy:** PII Inventory and Security Breach Procedures:
  
  http://its.ucsc.edu/policies/breach-procedures.html

- **ITS Policy:** regarding storage and transmission of PII (see slide 64):
  
  http://its.ucsc.edu/policies/pii.html

- **UCSC PII Resources:** http://its.ucsc.edu/security/pii.html
Credit Card Data

The protection of credit card information is regulated by the Payment Card Industry Data Security Standard (PCI DSS).

At UCSC, the Campus Controller governs compliance with the PCI DSS. Detailed information about the PCI DSS is available at https://www.pcisecuritystandards.org/security_standards/index.php

ITS staff who administer systems or applications that store, process or transmit credit card data are expected to be familiar with and follow the PCI DSS requirements (available from the above web page) as applicable to the environment they administer, and to participate in the campus PCI compliance process as needed. Additional training is also required: http://its.ucsc.edu/security/training/its-staff.html#pci.
Definitions, cont. (5 of 8)

Electronic Protected Health Information (ePHI)
Also known as “HIPAA Data”

E PHI is patient health information which is computer based, e.g., created, received, stored, maintained, processed, and/or transmitted in electronic media. Examples include:

- Medical record number, account number, or SSN
- Patient demographic data, e.g., address, date of birth, date of death, sex, email / web address
- Dates of service, e.g., date of admission, discharge
- Medical records, reports, test results, appointment dates
More on ePHI / HIPAA Data:

E PHI is regulated by federal and state laws, UC policy and UCSC policy.

At UCSC, the Information Security Officer (ISO) is responsible for compliance with security-related laws and policies governing ePHI. The Executive Director of the Student Health Center is responsible for compliance with privacy-related laws and policies governing this information.

Everyone with access to ePHI or HIPAA systems must complete HIPAA training.

Detailed information and links to training are available at http://its.ucsc.edu/policies/hipaa.html

The disclosure of information from student records is governed by FERPA. Even though most student records are not considered restricted data, it’s important to know about rules governing their disclosure.

Confidential information from student records may not be shared or disclosed beyond “business need to know” within the University.

At UCSC, the Registrar is the authoritative office for FERPA. Refer to the Registrar's website for information about privacy requirements for student records, as well as related resources:
http://registrar.ucsc.edu/records/privacy/

Everyone with access to FERPA-protected data should review this website and complete the Registrar's FERPA quiz (also at the above link).
Definitions, cont. (8 of 8)

More on FERPA:

**All** information for students with a Non-Release of Public Information (NRI/FERPA flag) in the Academic Information System (AIS) is considered confidential, including the fact that they are a student.

*Note: There is no equivalent to an NRI flag for staff or faculty.*

**Student records are protected by both Federal and State laws:**

The disclosure of information from student records is governed both by FERPA and the State of California Education Code.

Potential consequences for violations include legal or civil action and withdrawal of funds under any program administered by the Secretary of Education.
A word about notifying people in the event of a security breach

As mentioned earlier, state law requires us to notify people if there is a reasonable belief that their PII has been accessed without authorization.

Even if notification is not required by law, various factors can affect a decision to notify or not notify people of a security breach. These include:

- The scale of the breach/number of people affected
- The potential for harm given the type(s) of information breached
- The potential for negative publicity if we didn’t notify and the breach were discovered by someone affected or by the media
- The likelihood that someone will actually be able to use the information to cause harm
- An assessment of whether notifying people could potentially cause more harm than good given the circumstances
Requirement to notify people when their personal information is collected, and to provide an opt-out

The UC Electronic Communications Policy (ECP) requires people be informed whenever personally identifiable information other than *transactional information* is collected and stored automatically by a system or service. This applies to any information that identifies or describes an individual, not just PII, as defined earlier in this section. This can be accomplished, for example, by a notice on the login screen or on individual pages of an application or web site, along with a description of how the information may be used.

In addition, users should be able to terminate an electronic communications transaction without leaving personal data. This is a requirement for systems and services in which the University is a partner with a state agency or the California State University.

*See Glossary for definition: [http://its.ucsc.edu/policies/glossary.html](http://its.ucsc.edu/policies/glossary.html)
Topics

- IT Service Provider Responsibilities
- Access Principles
- Sensitive Data: Definitions and Protection
- Key Security Practices for IT Service Providers
- Acceptable Use and Personal Use
- Reporting Security Incidents
- Additional Resources;
  Appendices: List of Links and List of Contacts
- Test Your Understanding
Privileged Access Increases the Stakes for Security Glitches and Slip-Ups

The stakes are higher if someone gets into one of your systems, or gets hold of your passwords.

You need to be *more* aware than most people about security risks and *more* careful about protection.
Beware of Social Engineering

Social Engineering is the practice of obtaining access credentials or confidential information by tricking or manipulating legitimate users.

- Don’t be fooled. Always verify the identity of individuals requesting passwords, password resets, access codes, sensitive information, information about a secure facility, or entry to a secure area.
  - Even if they say it’s an emergency
  - Even if they say they are the Chancellor or the campus Police Chief.
  - ITS leadership will support you if you need to delay fulfilling a request until its legitimacy can be verified

- Don’t fall for “click on this link,” “open this attachment,” “forward this email,” “confirm your information,” or “install this plugin” scams.
  - Your first reaction should always be to be skeptical.
  - You can also check an urban legend site such as Snopes to find out whether you are looking at a known scam.
Password Requirements (1 of 4)

All passwords used by ITS staff must comply with the campus Password Standards. These Standards are requirements for passwords that provide access to restricted data (covered earlier in this training).

The campus Password Standards are available at http://its.ucsc.edu/policies/password.html. Some reminders include:

- Use strong passwords.
- Don’t share or disclose your passwords.
- Don’t let applications or web browsers stores/“remember” passwords that provide access to restricted data or systems.
- Store and transmit passwords securely. Electronically stored passwords should be encrypted.
Password Requirements (2 of 4)

The Password Standards identify a number of specific IT Service Provider responsibilities in addition to general strength and security requirements:

1. Initial passwords and password resets should meet the Password Standards. They should also not be a fixed password or a published/easy-to-figure-out formula.

2. Educate end users about the password standards, especially when it is not possible for applications and systems to enforce them technically.

3. Ensure secure transmission and storage of passwords.

4. Give users advance notice about password requirements so they can come up with well thought out, memorable passwords instead of spur-of-the-moment ones.

5. Passwords used for privileged access (defined in section 1 of this training) should be different than those for non-privileged access.

This is an abbreviated list. Please refer to the Password Standards for more detailed information: http://its.ucsc.edu/policies/password.html
Password Requirements (3 of 4)

The Password Standards also identify a number of technical requirements and standards
(abbreviated list – see Sec V at http://its.ucsc.edu/policies/password.html)

1. Applications and systems should be configured to:
   - enforce the password standards where possible and applicable
   - ensure secure transmission and storage of passwords
   - prevent resubmission of previously used passwords

2. Passwords provided for initial access and password resets should be unique. They should also be set to expire upon initial use, where feasible.

3. All default passwords for network-accessible device accounts should be modified.

4. New systems and applications should be able to support the password standards.
Password Requirements (4 of 4)

Authentication
- Always verify a person’s identity before providing an account or password to them, regardless of how the request is received (in person, online, IT Request, phone, email, etc.)
  - Or make sure applications include a verification mechanism
  - This includes password resets

Delivery
- Passwords should be transmitted securely
  - Not via unencrypted email or IM
    - If you have to use email or paper mail, it’s best to send the username and password separately.
  - Avoid including passwords in IT Request tickets, since they are emailed and the password is retained in the ticket. Use a more secure delivery method whenever possible.
- Printed passwords should be stored securely while awaiting delivery or pickup
Reminder about Privileged and Admin Accounts

Remember that it is especially important to follow good security practices for privileged and admin-level accounts. For example,

- Log out of these accounts/terminate sessions when you’re not using them – and make sure a strong password is required to re-connect.

- You should have to enter your password each time you connect to a privileged or admin-level account. Don’t let applications or shortcuts remember or cache your login information.

- Use your own, unique login whenever possible and elevate privileges. Use sudo, “run as,” etc. instead of accessing admin accounts or root directly.

- Passwords used for privileged/admin-level access should be different than those for “regular” access.
Other Key Security Measures for IT Service Providers (1 of 4)

- Don’t let your computer get infected or hacked
  - Make sure OSes and applications are patched and up-to-date
  - Make sure anti-virus/anti-malware is installed, running, and up-to-date
  - Don’t install unknown or unsolicited programs on your computer
  - Don’t click on unknown or unsolicited links in spam, email, popups, IM, Facebook, Twitter, blogs, texts, etc.
  - Don’t open unknown or unsolicited attachments
  - Don’t open files sent via IM
  - Set up your browsers according to ITS’ Secure Browser Settings: http://its.ucsc.edu/software/release/browser-secure.html
  
  Note: these are required for HIPAA workstations

- Use caution when punching holes in firewalls – don’t break our security model
Other Key Security Measures for IT Service Providers (2 of 4)

- Send restricted data securely
  - Don’t use email unless it is encrypted
  - Never send restricted data via instant message (IM)

- Shut down, lock, log off, or put computers to sleep before leaving them unattended – and make sure they require a password to start up or wake up
  - As a back-up, set your computer to auto-lock or go to screensaver when inactive for longer than 20 minutes (10 minutes max for HIPAA machines).

- Terminate sessions when you’re done, or set them to time-out. Make sure a password is required to re-connect.
Other Key Security Measures for IT Service Providers (3 of 4)

- Close up and lock secure areas before leaving them unattended – even just for a minute
  - Don’t share your lock code or key, and don’t hold locked doors open for unknown people
- Protect laptops and other portable devices
  - Lock them down, lock them up, or take them with you – at work and away from work.
  - Don’t keep sensitive information or your only copy of critical data, projects, files, etc. on portable devices unless they are properly protected
    - Even if it’s only on there temporarily, or you’re just transporting the data from one place to another, or just doing a restore
Other Key Security Measures for IT Service Providers (4 of 4)

- Don’t leave equipment, CDs, passwords, sensitive papers, etc. lying around unattended
  - Including in your office, on printers, fax machines, copiers, in mailrooms, etc.
  - Remember to put these items away and lock them up before you leave a shared or unsecured location
  - For those of you who work at 2300 Delaware, keep in mind that it is not a secure work environment – assume it could be stolen if it is left out (whatever “it” is)

- See ITS’ Security website for additional details and practices: http://its.ucsc.edu/security/
UCSC’s Minimum Network Connectivity Requirements Policy

UCSC’s Minimum Network Connectivity Requirements Policy, available at http://policy.ucsc.edu/policies/its/it0004.html, identifies minimum security requirements for devices connected to the campus network. These are summarized on the next slide. ITS employees are expected to ensure that devices for which they are responsible comply with these requirements. Some of the “Key Security Measures” on the previous pages are from this policy.

According to the IT Security Team, if the campus adhered to the Minimum Network Connectivity Requirements, most of the security issues they see would be addressed.

Information designed to help clients understand and meet these requirements is available at http://its.ucsc.edu/security/stay-secure.html

Campus information security requirements apply to all devices used for University business purposes, regardless of ownership or location.
Summary of Minimum Network Connectivity Requirements

1. Shared-access systems must use passwords or other access controls.
2. Passwords must comply with campus password requirements (see slides 48-50).
3. Passwords must be encrypted when transmitted.
4. Networked devices must run operating system and application software for which security patches are made available. Patches should be installed in a timely fashion.
5. Use malicious software protection – required for both PCs and Macs.
6. Remove, turn off, or disable unnecessary services.
7. Use a host-based firewall if available.
8. Unauthenticated or unauthorized email relays or proxy servers are not allowed.
9. Session/screensaver timeout is required for devices that access restricted and/or essential resources.
10. Based on level of risk, UCSC may require that computers run a security audit agent as a condition for attaching to the campus network.

This is only a summary. Please refer to the policy for more detailed information: http://policy.ucsc.edu/policies/its/it0004.html
Additional Considerations for Protecting Restricted Data (1 of 4)

1. Keep restricted data to a minimum. The less we have, the lower the risk. The best way to protect restricted data is not to have it in the first place, or to have it in the fewest places possible, if you have to have it.

- Truncate, de-identify or redact restricted data elements whenever possible.
- Securely delete restricted data that is no longer needed – and remember to shred hard copies.
- This includes data in dev, test, training, or bug systems.
- Clean devices before disposal or re-purposing.
  - Including hard-drives, CDs, zip disks, flash drives, back-up tapes, printer hard drives, etc.
Additional Considerations for Protecting Restricted Data (2 of 4)

2. **Know where this data exists** – who has access to it, where and how it is displayed, what is available via queries, etc.
   - This is important to keep in mind up front as user interfaces are being designed.
   - Restricted data can be in current or old files, including backups, transactional logs, and archives.
   - Restricted data can also be on laptops, home machines, portable devices, etc.

3. **Make sure restricted data isn’t stored in locations with broader access rights than appropriate**
   - And make sure it isn’t publicly accessible online (even if the URL isn’t linked from anything)
4. **Ensure appropriate system security**
   - Restricted data must be stored securely wherever it lives, including in dev, test, training, and bug tracking systems.
     - It should be encrypted where possible and practical.
     - This includes home machines, portable devices, and laptops.
     - Unencrypted ePHI may not be stored on portable devices.
     - Restricted data **must** be encrypted if stored in Google or any other non-UCSC service.
   - Consider having employees use a secure server instead of local drives or the cloud for storing restricted data.

5. **Restricted data must be encrypted when transmitted**
   - Either the data itself must be encrypted before it is sent or the transmission channel must be encrypted, or both.
   - This also applies to printing, remote access, transmission of backups, transmission of “real” test or dev results and data.
   - See [http://its.ucsc.edu/certificates/](http://its.ucsc.edu/certificates/) for UCSC’s Digital Certificate Service
Additional Considerations for Protecting Restricted Data (4 of 4)

6. All access to restricted data should be traceable to individuals. This means issuing and using unique access credentials, not shared accounts, whenever possible for access to restricted data.
   - As mentioned earlier in this training, use your own, unique login whenever possible and elevate privileges instead of accessing admin accounts or root directly.

7. Set up your workstation so that unauthorized people and passers-by cannot see the information on your monitor.

→ Additional information about protecting restricted data is available at http://its.ucsc.edu/policies/rdpp.html
What’s Not OK to Have on a Laptop, Portable Device, or Unencrypted Drive?

- ITS employees are not to store unencrypted personal identity information (PII) on portable devices. See full policy on the next slide.

- Per campus policy, unencrypted electronic protected health information (ePHI/HIPAA data) may not be stored on portable devices, including laptops. See definition of ePHI earlier in this training.

- If the device were stolen, would it be a problem if the data fell into a malicious person’s hands? If the answer is yes, don’t store it unencrypted on a laptop or other portable device.

- Servers and other non-portable devices that contain restricted data need to be physically secure, and the data should still be encrypted where possible and practical.

- Unencrypted backups containing restricted data must be stored securely.
ITS Policy on Storage and Transmission of Personal Identity Information (PII)

The following is ITS’ Divisional policy regarding storage and transmission of personal identity information (PII). While these practices are encouraged for all PII, this policy specifically applies to ITS employees and their individual use of PII in the course of their jobs.

1. ITS employees must limit their own storage of PII to the minimum amount necessary, guided by law and policy.

2. ITS employees are not to download unencrypted PII to portable devices or media such as mobile phones, tablets, USB drives, external hard drives, and CDs/DVDs.

3. As a general rule, PII should be stored on secure servers. If an ITS employee must temporarily store unencrypted PII on his or her desktop or laptop computer, it should be encrypted and securely deleted as soon as possible. If an ITS employee must temporarily store unencrypted PII on his or her desktop or laptop computer, it must be securely erased on a daily basis.

4. PII must be transmitted securely. Additionally, ITS employees are not to send PII in unencrypted email or via unencrypted instant messaging (IM) or texts.

5. PII and other restricted data must be encrypted if stored in Google or any other non-UCSC service.

6. ITS employees are not to store or access PII on a non-University device.

The full policy is at http://its.ucsc.edu/policies/pii.html. See slide 35 for a definition of PII. Additional information about PII, including information about securely deleting files, is available at http://its.ucsc.edu/security/pii.html.
Non-University Devices & Working Remotely

Campus information security requirements apply to all devices used for University business purposes, regardless of ownership or location.

Restricted data still needs to be protected, passwords need to be sent securely, computers need to be protected against intruders and hackers, etc.

It is important to assess your remote work and use of non-University devices to ensure that necessary security is not overlooked. This may mean taking extra precautions or not doing certain tasks on mobile devices or shared or public machines, including home computers, if you’re not able to ensure proper security such as UCSC’s Minimum Network Connectivity Requirements (see slides 57-58).

Please refer to UCSC’s Remote Access Requirements for additional guidance: http://its.ucsc.edu/policies/ra.html. Also keep in mind ITS’ Policy on Storage and Transmission of PII (see previous slide).
A Special Word about Mobile Devices

- Don’t store sensitive information on portable devices. Turn on encryption if you do.
- Set your device to require a password/PIN (a complex one, if possible) and to automatically lock when not in use – but still don’t store anything you’re not willing to lose.
- Some devices can be erased remotely, or can erase themselves if the password/PIN is entered incorrectly a certain number of times. Consider turning these features on to protect information in the case of theft or loss.
- Set devices to “ask” before joining networks so know what you’re connecting to.
- Avoid using auto-complete features that remember user names or passwords.
- Avoid opening files, clicking links, or calling numbers in unsolicited emails, texts, or IMs.
- If your device has a web browser, set the browser to block pop-ups. For added privacy, also set the browser to limit the cookies it accepts.
- Delete all contents before discarding, exchanging, selling, or donating the device.
- Back up your data regularly in case of theft or loss.
- **Immediately report lost or stolen devices that contained sensitive UCSC information or passwords** to the ITS Support Center (see “Reporting Security Incidents,” slides 76-78).
- See [http://its.ucsc.edu/security/mobile.html](http://its.ucsc.edu/security/mobile.html) for additional information about protecting mobile devices, including a checklist for lost/stolen devices and precautions in case of theft/loss.
Working with Test, Dev and Training Systems

When possible, don’t include restricted data in development, testing or training systems.

- Restricted data in these systems needs to be protected just like any other restricted data, both in storage and transmission
  - This includes bug tracking systems and bug reports

- Consider truncating, redacting, or de-identifying restricted data, using fake data, encrypting or deleting columns or tables, etc.
Account Authorization and Review

- Ensure appropriate authorization before providing access to restricted data – *especially* privileged access.
  - It’s also important to ensure that the approver understands the type and level of access they’re granting.

- **ITS supervisors:** You are responsible for prompt modification or termination of accounts for your staff when job duties change or end.
  - Always use ITS’ offboarding checklist when employees leave: [http://its.ucsc.edu/internal/supervisor-resource.html#offboard](http://its.ucsc.edu/internal/supervisor-resource.html#offboard)
  - Admin-level access should be removed within one business day.
  - Root and shared admin passwords must be changed when someone with access to them leaves or should no longer have access.
  - Cancel or change door lock codes, including shared codes.
Log Review and Backup Retention

Log Review:
- Logging must be enabled at the operating system, application/database, and system/workstation level on resources that contain, access or transmit confidential or restricted data.
- Logs must be reviewed in response to suspected or reported security problems and as requested by IT Security. Proactive log review may also be required by the System Steward/Data Owner.
- UCSC Log Policy: [http://policy.ucsc.edu/policies/its/it0005.html](http://policy.ucsc.edu/policies/its/it0005.html)
- UCSC Log Procedures: [http://its.ucsc.edu/policies/log-procedures.html](http://its.ucsc.edu/policies/log-procedures.html)

Backup Retention:
- The Data Center Backup Service service page describes the retention schedule for backups created and managed by the Data Center: [http://its.ucsc.edu/data-center/backups.html](http://its.ucsc.edu/data-center/backups.html) (under “Features and Benefits”).
Working with Third-Parties: Vendors, Contractors and Service Providers

It is important to make sure non-UC vendors, contractors and service providers protect University systems and data to which they have access.

- Data security contract language must be in place for third-parties with access to confidential data. UCSC has standard contract language for this.
  - Check with Purchasing to make sure this language is included in agreements and purchase orders that involve confidential or restricted data.
  - Additional processing time may be needed for these agreements.
  - Purchasing and Business Contracts consult with the campus Information Security Officer (ISO) on all agreements that would provide a third party with access to restricted data.
  - Certain types of data, such as HIPAA or credit card data, require additional agreements. Notify Purchasing if this applies.
- Make sure third-parties understand the nature of the data and systems they have access to, and any security requirements and expectations.
- Additional information: [http://its.ucsc.edu/security/appendixds.html](http://its.ucsc.edu/security/appendixds.html)
Emergency Procedures

- Do not put yourself in personal danger during emergencies.
- Log out of systems that contain restricted data, secure files, and lock up before evacuating a building, if it is safe to do so.
- Upon re-entry after an evacuation, check your area to ensure there is no evidence of tampering or unauthorized access. Verify security controls are functioning as expected. Report anomalies as a potential security incident.
- Default procedures for providing access to systems or data under emergency circumstances:
  - Follow standard, business-as-usual, operating procedures for access authorization and provision if possible.
  - Follow instructions from the ITS Division Operation Center (DOC) Manager, if it has been activated. ITS DOC information: http://its.ucsc.edu/change-mgmt/its-doc.html
  - If the DOC has not been activated and it is not possible or practical to follow standard operating procedures, escalate emergency requests for access to an ITS Director or the VC IT for direction or possible DOC activation.
Topics

- IT Service Provider Responsibilities
- Access Principles
- Sensitive Data: Definitions and Protection
- Key Security Practices for IT Service Providers
- **Acceptable Use and Personal Use**
- Reporting Security Incidents
- Additional Resources; Appendices: List of Links and List of Contacts
- Test Your Understanding
Acceptable Use of UCSC IT Resources

In general, acceptable use of UCSC IT resources meets the following criteria:

- There is a legitimate business need
- It doesn’t introduce a security risk
- It doesn’t interfere with or disrupt normal operations, or create an excessive burden on campus systems or resources
- It’s legal and does not violate UC or UCSC policy
- It doesn’t interfere with job duties or create a hostile working or learning environment
- It doesn’t inappropriately imply University representation or endorsement.

This is only a summary. UCSC’s Acceptable Use Policy is available at http://policy.ucsc.edu/policies/its/it0003.html
Personal Use of UC IT Resources

University IT resources are to be used for University business purposes. It is OK to use them for incidental personal purposes as long as the use complies with UCSC’s Acceptable Use Policy (see previous slide), all of the provisions of the UC Electronic Communications Policy* and UC Business and Finance Bulletin G-46**, and does not:

- interfere with the user’s employment or other obligations to the University,
- burden the University with noticeable incremental costs,
- include use for commercial purposes not under the auspices of the University,
- include use for personal financial gain except as permitted under applicable academic personnel policies,
- inappropriately imply University representation or endorsement.

It is important to note that records resulting from incidental personal use of University resources may be designated University records subject to disclosure to the University and third parties in accordance with law.

* UC ECP: http://policy.ucop.edu/doc/7000470
** UC BFB G-46: http://policy.ucop.edu/doc/3420357
Topics

- IT Service Provider Responsibilities
- Access Principles
- Sensitive Data: Definitions and Protection
- Key Security Practices for IT Service Providers
- Acceptable Use and Personal Use
- **Reporting Security Incidents**
- Additional Resources;
  Appendices: List of Links and List of Contacts
- Test Your Understanding
What is a Security Incident?

A security incident is any attempted or successful unauthorized access, disclosure, or misuse of computing systems, data or networks, including theft and hacking.

If a computer has been lost or you suspect it may have been compromised, ask if it contains or accesses restricted data. Give examples (see slide 32) to make sure nothing is overlooked. Be sure to include this information in your report (see next two slides).

High-security systems, e.g. PII, HIPAA, PCI, or FERPA, (see slides 35-42) that are not configured according to established security requirements should be treated as potential security incidents and investigated.
Reporting Security Incidents

- Report lost or missing computing equipment to the police and your supervisor.
  - On-campus theft: Contact the UCSC Police Department at 459-2231 or http://police.ucsc.edu/
  - Off-campus theft: Contact local police
  - Open an IT Request ticket and cc/watchlist security@ucsc.edu if the device contained restricted or FERPA-protected data, or passwords

- Immediately report other suspected security incidents and breaches to your supervisor and the ITS Support Center (open an IT Request ticket), and cc/watchlist security@ucsc.edu.
  - If applicable, also notify the System Steward, departmental manager or ITS Divisional Liaison for the affected system or data
  - Always say whether the system is used for restricted data
  - When responding to a potentially compromised computer, follow ITS’ “Compromised Computer Procedures” at http://its.ucsc.edu/policies/compromise.html
Campus Incident Response Procedures

If you report a security incident involving restricted data, be sure to cc/watchlist security@ucsc.edu. IT Security will contact you with instructions. You may also be asked to help complete an Initial Incident Report.

- **Do not take any other action** (e.g. patching or rebuilding the system, running anti-virus, etc.) **before hearing from IT Security**; it may compromise a technical investigation.

- More detailed security incident procedures are included in UCSC’s *PII Inventory and Security Breach Procedures, Sec. V*: [http://its.ucsc.edu/policies/breach-procedures.html#breach](http://its.ucsc.edu/policies/breach-procedures.html#breach)

- Complex or severe security incidents may result in the activation of a security-focused DOC: [http://its.ucsc.edu/change-mgmt/its-doc.html](http://its.ucsc.edu/change-mgmt/its-doc.html)
Report Suspicious Activity to the Police

In addition to reporting suspected theft of UCSC-related computing equipment to the police (see slide 77), certain types of suspicious activities should also be reported to the police. Campus police: 911, 459-2231 or http://police.ucsc.edu/

Examples of suspicious activity to report to the police include:

- A person loitering in front of a building or near a secure area at unusual hours.
- Anyone tampering with or forcing entry into a building or vehicle.
- A person who is running and does not appear to be exercising, especially if carrying property could be fleeing the scene of a crime.
- Simply carrying property may be regarded as suspicious if it is at an unusual hour, in an unusual place, or if the person appears to be trying to conceal the property.
- Open or broken windows and doors at a home or business could mean a burglary still in-progress or already completed.
- Any vehicle without lights at night, cruising slowly, or following a course that seems aimless or repetitive.
- Persons claiming to be representatives of utilities (gas, phone, water, electric, cable), or even from campus services, but who are not in uniform or have no company identification may be burglars.
Checking for Lost or Stolen Devices on the Network

Requests for ITS staff to check whether a lost or stolen device has connected to our campus network must come from campus police. Please direct people who want us to look for their lost/stolen device to the campus police: http://police.ucsc.edu/ or 9-2231.

- ITS has also developed a checklist to help people with lost or stolen mobile devices:
  http://its.ucsc.edu/security/mobile.html#list
  Please refer people to this checklist as appropriate.
Reporting Privacy Incidents

Report suspected privacy violations, such as inappropriate disclosure or access of information, to UCSC’s Privacy Official:

- Email: privacy@ucsc.edu
- Phone: 831-459-4003
- Campus Privacy Website: http://privacy.ucsc.edu/
Topics

- IT Service Provider Responsibilities
- Access Principles
- Sensitive Data: Definitions and Protection
- Key Security Practices for IT Service Providers
- Acceptable Use and Personal Use
- Reporting Security Incidents

- Additional Resources;
  Appendices: List of Links and List of Contacts

- Test Your Understanding
Additional Resources

Security Awareness:

- ITS Security website
  http://its.ucsc.edu/security/
  - "Top 10 List" of Good Computing Practices
  - PII and Restricted Data resources
  - Minimum Network Connectivity Requirements
  - Cyber Security Basics
  - Computer security training and tutorials
  - How to report computer security incidents
  - Copyright education website
  - Links to alerts and related resources, policies and procedures

IT-Related Policies, Practices, Guidelines:

- ITS Security Policy website: http://its.ucsc.edu/policies/
State Laws

- California Civil Code 1798.29, which requires us to notify people if their unencrypted PII is disclosed without authorization:
  [http://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=CIV&division=3.&title=1.8.&part=4.&chapter=1.&article=7](http://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=CIV&division=3.&title=1.8.&part=4.&chapter=1.&article=7)

UC Policies

- UC Electronic Communications Policy. Includes policy for routine monitoring activities (Sec IV.C 2.b and V.B):
  [http://policy.ucop.edu/doc/7000470](http://policy.ucop.edu/doc/7000470)

- UC BFB G-46, Guidelines for the Purchase and Use of Cellular Phones and Other Portable Electronic Resources:
  [http://policy.ucop.edu/doc/3420357](http://policy.ucop.edu/doc/3420357)

- UC BFB IS-3, Electronic Information Security:
  [http://policy.ucop.edu/doc/7000543](http://policy.ucop.edu/doc/7000543)
Appendix 1: List of Links (2 of 3)

UCSC Policies
- Acceptable Use Policy: http://policy.ucsc.edu/policies/its/it0003.html
- ITS Policy regarding storage and transmission of PII: http://its.ucsc.edu/policies/pii.html
- Log Policy: http://policy.ucsc.edu/policies/its/it0005.html
- Minimum Network Connectivity Requirements: http://policy.ucsc.edu/policies/its/it0004.html
- Password Standards: http://its.ucsc.edu/policies/password.html
- PII Inventory and Security Breach Procedures: http://its.ucsc.edu/policies/breach-procedures.html
- Remote Access Requirements: http://its.ucsc.edu/policies/ra.html
- UCSC Implementation of the UC Electronic Communications Policy: http://its.ucsc.edu/policies/ecpi.html
Appendix 1: List of Links (3 of 3)

Resources

- Access to Information Statement: http://its.ucsc.edu/accounts/docs/access-info-stmt.pdf
- Compromised Computer Procedures: http://its.ucsc.edu/policies/compromise.html
- Data security contract language: http://its.ucsc.edu/security/appendixds.html
- Digital Certificate Service: http://its.ucsc.edu/certificates/
- Glossary of policy terms: http://its.ucsc.edu/policies/glossary.html
- HIPAA web site: http://its.ucsc.edu/policies/hipaa.html
- ITS DOC: http://its.ucsc.edu/change-mgmt/its-doc.html
- ITS on/offboarding checklists: http://its.ucsc.edu/internal/supervisor-resource.html#onboard
- PCI DSS web site: https://www.pcisecuritystandards.org/security_standards/index.php
- PII resources: http://its.ucsc.edu/security/pii.html
- Records Access Notice: http://its.ucsc.edu/policies/access-notice.html
- Registrar’s FERPA web site: http://registrar.ucsc.edu/records/privacy/index.html
- Routine monitoring practices: http://its.ucsc.edu/policies/monitoring.html
- Secure Browser Settings: http://its.ucsc.edu/software/release/browser-secure.html
- Security web site: http://its.ucsc.edu/security/
Appendix 2: List of Contacts

- Campus Counsel: 459-1848, campuscounsel@ucsc.edu
- IT policy office (Janine and Julie): 459-2779, itpolicy@ucsc.edu
- IT Security List: security@ucsc.edu
- ITS Divisional Liaisons: http://its.ucsc.edu/get-help/dls.html
- Whistleblower Office: http://whistleblower.ucsc.edu/
Topics

- IT Service Provider Responsibilities
- Access Principles
- Sensitive Data: Definitions and Protection
- Key Security Practices for IT Service Providers
- Acceptable Use and Personal Use
- Reporting Security Incidents
- Additional Resources; Appendices: List of Links and List of Contacts

- Test Your Understanding
Test Your Understanding
**Question 1**

A parent calls the Support Center trying to locate her son. She heard he is working at UCSC. You have access to PPS and verified that he works for Shakespeare Santa Cruz. What should you do?

A. Hang up

B. Tell the parent her son works for Shakespeare Santa Cruz, but don’t provide any additional information

C. Refer the parent to Staff Human Resources

D. Answer all the parent’s job-related questions; employment at UC is public information
Answer 1

A parent calls the Support Center trying to locate her son. She heard he is working at UCSC. You have access to PPS and verified that he works for Shakespeare Santa Cruz. What should you do?

C. Refer the parent to Staff Human Resources

Even though certain employment information at UC is public information and the Support Center can see the requested information in PPS, that is not the purpose for which the Support Center was granted access to PPS. It is only OK to use your access for the purposes for which it was granted.

See slides 14 and 19 for additional information.
Question 2

Which of the following is part of UCSC’s minimum network connectivity requirements?

A. Don't install unknown or unsolicited programs on your computer.

B. Make backup copies of files or data you are not willing to lose.

C. Make sure your computer is protected with anti-virus and all necessary security patches and updates.

D. Shut down, lock, log off, or put your computer to sleep before leaving it unattended.
Answer 2

Which of the following is part of UCSC’s minimum network connectivity requirements?

C. Make sure your computer is protected with anti-virus and all necessary security patches and updates.

The other answers are all good computing practices but are not actually minimum network connectivity requirements.

See slide 57-58 for additional information.
Question 3

Which of the following is NOT always considered “restricted data” at UCSC?

A. Personal Identity Information (PII)
B. Court-ordered settlement agreements requiring non-disclosure
C. Credit card data regulated by the Payment Card Industry (PCI)
D. Home address and home telephone number
E. Information relating to an ongoing criminal investigation
Answer 3

Which of the following is NOT always considered “restricted data” at UCSC?

D. Home address and home telephone number

Individual units/departments have the ability to elevate any information they deem sensitive enough to the level of restricted data, but home address and home telephone number are not on the list of types of information that UCSC automatically considers to be restricted data.

See slides 31-34 for additional information.
Question 4

You should begin using your access to privileged systems as soon as you receive your login information.

A. True
B. False
Answer 4

You should begin using your access to privileged systems as soon as you receive your login information.

B. False

You must receive appropriate authorization and training before making use of privileged access – even if the account is all set up and ready to go.

See slide 9 for additional information
Question 5

When investigating a possible computer security incident, always (select all that apply)

A. If malware is involved, take the system offline and rebuild it immediately
B. Notify the ITS Support Center
C. Notify campus police
D. Ask if the system contained or accessed restricted data
E. Complete an Initial Incident Report
F. All of the above
Answer 5

When investigating a possible computer security incident, always (select all that apply)

B. Notify the ITS Support Center
D. Ask if the system contained or accessed restricted data

The other answers may be appropriate under certain circumstances, but the above answers are the only ones that always apply.

See slides 76-78 for additional information
Question 6

Which of the following is an example of student information that is always considered confidential under FERPA?

A. Mailing address
B. Major
C. GPA
D. Degrees received
Answer 6

Which of the following is an example of student information that is always considered confidential under FERPA?

**C. GPA**

*GPA is considered confidential even if a student hasn’t elected “non-release of information” (NRI) in AIS.*

*See slides 41-42 for additional information*
Question 7

Your co-worker asks for your password so he can look at a file on your computer. You want him to see the file, so you should give him your password.

A. True
B. False
Answer 7

Your co-worker asks for your password so he can look at a file on your computer. You want him to see the file, so you should give him your password.

B. False

Don’t share your password, even if it seems innocent. Find another way to get the file to your co-worker.

See slide 48 for additional information
Question 8

One of the Deans approaches a LITS and requests immediate access to the email and files of an employee who is on leave. The Dean explains that the email/files are needed to continue business in the employee’s absence. What should the LITS do?

A. Provide the access. The Dean is authorizing it.
B. Go through the employee’s email and files one-by-one and forward the ones the Dean says are needed.
C. Have the Dean or someone from the department ask the employee for permission. If the person can’t be reached, explain the access without consent process.
D. Explain that ITS has no way to access an individual’s email or files.
Answer 8

One of the Deans approaches a LITS and requests immediate access to the email and files of an employee who is on leave. The Dean explains that the email/files are needed to continue business in the employee’s absence. What should the LITS do?

C. Have the Dean or department ask the employee for permission. If the person can’t be reached, explain the “access without consent” process.

An individual’s permission is required to access their electronic communications records. Vice Chancellor-level authorization is required for nonconsensual access to someone’s records – even by ITS staff – so the Dean can’t authorize this access.

See slides 16-20 (including the link on slide 17) for additional information.
Question 9

Which of the following are examples of acceptable personal use of UC IT resources? (select all that apply)

A. Emailing potential donors about your child’s school fundraiser
B. Calling your dentist from your work phone to change an appointment
C. Checking online for a weather report
D. Including the website for your family’s business in your UCSC email signature
E. None of the above
Answer 9

Which of the following are examples of acceptable personal use of UC IT resources? (select all that apply)

B. Calling your dentist from your work phone to change an appointment

C. Checking online for a weather report

UC policy allows incidental personal use of University IT resources. These resources may not, however, be used for non-University commercial purposes or personal financial gain and must not inappropriately imply University representation or endorsement.

See slide 74 for additional information
Question 10

Which of the following is true when working remotely?

A. As long as you work quickly, the risk is minimal

B. Some tasks should not be done on public computers if security can’t be ensured

C. It’s best to save a copy of the information you need on your home computer because it is risky to download it

D. None of the above
Answer 10

Which of the following is true when working remotely?

B. Some tasks should not be done on public computers if security can’t be ensured.

Sensitive information needs to be protected at all times, regardless of your work location. If you can’t guarantee the security of the computer or transmission, don’t work with sensitive information. This includes home computers and wireless.

See slide 65 for additional information.
Question 11

You receive a call from an employee in the Chancellors office requesting a password reset. You are familiar with the name and know that the person really does work in the Chancellors office. You should:

A. Reset the password.
B. Confirm the caller’s identity before resetting the password.
C. Reset the password immediately if the caller says it is urgent, but be sure to confirm the caller’s identity later.
D. None of the above.
Answer 11

You receive a call from an employee in the Chancellors office requesting a password reset. You are familiar with the name and know that the person really does work in the Chancellors office. You should:

B. Confirm the caller’s identity before resetting the password.

Don’t fall for social engineering tricks. Always verify a person’s identity before acting on requests for passwords, password resets, access codes, entry to a secure area, or sensitive information.

See slide 47 and 51 for additional information.
Question 12

Which of the following passwords meets UCSC’s password requirements?

A. @#$)*&^%
B. akHGksmLN
C. UcSc4Evr!
D. Password1
Answer 12

Which of the following passwords meets UCSC’s password requirements?

C. UcSc4Evr!

This is the only choice that meets all of the following UCSC requirements:

- At least 8 characters in length
- Contains at least 3 of the following 4 types of characters: lower case letters, upper case letters, numbers, special characters
- Not a single word preceded or followed by a digit

See slide 48 (Password Standards link) for additional information
Question 13

A supervisor asks you to check an employee’s browser history to determine if the employee has been goofing around at work. You should:

A. Do it
B. Refuse
C. Tell the supervisor to get the employee’s permission or go through the “access without consent” process
D. Install a keylogger on the employee’s computer so the supervisor can track the employee’s activities
Answer 13

A supervisor asks you to check an employee’s browser history to determine if the employee has been goofing around at work. You should:

C. Tell the supervisor to get the employee’s permission or go through the “access without consent” process

Browser history and other electronic records that can reveal information about someone’s activities or whereabouts is considered an electronic communications record. An individual’s permission or Vice Chancellor-level authorization is required to access these records.

See slides 16-19 (including the link on slide 17) for additional information
Questions?

Comments?

Please contact the ITS Service Manager for Policy and Compliance at 459-2779 or itpolicy@ucsc.edu
This is to certify that

________________________

has completed the online Computer Security and Policy Overview for IT Service Providers

Date: ________________

________________________  ________________________
Employee's Signature    Supervisor's Signature

ITS staff: Submit completed certificate to your supervisor. ITS supervisors: Place in employee file to document completion of training.