Today’s Agenda

- Data Governance Update
- Information Security Program Update
- Accessibility Update
Data Governance Update

Sandra Furuto, Data Governance Director
What is Data Governance

“...a framework that enables us to effectively manage data”

- Defines how data are collected, stored, and used
- Defines who can access data, when, and under what conditions
- Establishes decision rights
- Establishes clear lines of accountability
- Gives a voice to all appropriate parties
- Provides a mechanism for conflict resolutions involving data
UH Data Governance Goals

Protect the privacy and security of “Protected Data”
(all non-public data; includes Institutional Data and research data)

• Produce higher quality data for informed decision making
• Promote efficient use of resources
• Increase transparency and accountability
## EP2.214, Data Classification Categories

<table>
<thead>
<tr>
<th>Category</th>
<th>Definition</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public</td>
<td>Access is not restricted and is subject to open records requests</td>
<td>Student directory information, employee’s business contact info</td>
</tr>
<tr>
<td>Restricted</td>
<td>Used for UH business only; will not be distributed to external parties; released externally only under the terms of a written MOA or contract</td>
<td>Student contact information, UH ID number</td>
</tr>
<tr>
<td>Sensitive</td>
<td>Data subject to privacy considerations</td>
<td>Date of birth, job applicant records, salary/payroll information, most student information</td>
</tr>
<tr>
<td>Regulated</td>
<td>Inadvertent disclosure or inappropriate access requires a breach notification by law or is subject to financial fines</td>
<td>FN or first initial/LN in combination with SSN, driver license number, or bank information; credit card, HIPAA, or financial aid information</td>
</tr>
</tbody>
</table>
### Examples of Data / Information by Category

<table>
<thead>
<tr>
<th>Public</th>
<th>Restricted</th>
<th>Sensitive</th>
<th>Regulated</th>
</tr>
</thead>
<tbody>
<tr>
<td>Student Data</td>
<td>Student Data</td>
<td>Student Data</td>
<td>FN / first initial and LN with the following:</td>
</tr>
<tr>
<td>• Name</td>
<td>• UH email address/username</td>
<td>• Gender</td>
<td>• Social Security Number</td>
</tr>
<tr>
<td>• Major field of study</td>
<td>• Address (street name and number)</td>
<td>• Ethnicity</td>
<td>• Driver's license</td>
</tr>
<tr>
<td>• Class (i.e., freshman, sophomore, etc.)</td>
<td>• Personal phone number</td>
<td>• Grades</td>
<td>• Hawai‘i ID card number</td>
</tr>
<tr>
<td>Employee Data</td>
<td>Student &amp; Employee Data</td>
<td>Courses taken</td>
<td>• Financial account info, credit / debit card numbers, etc.</td>
</tr>
<tr>
<td>• Name</td>
<td>• UH ID number</td>
<td>GPA</td>
<td>Business/Financial Data</td>
</tr>
<tr>
<td>• Job title, description</td>
<td>• Banner PIDM</td>
<td>Employee Data</td>
<td>• Payment Card Industry Data</td>
</tr>
<tr>
<td>• Business address, phone number</td>
<td>• ODS PIDM</td>
<td>• Address (street name and number)</td>
<td>Security Standard (PCI-DSS) information</td>
</tr>
<tr>
<td>• Education and training background</td>
<td></td>
<td>• Personal phone number</td>
<td>Health Information</td>
</tr>
<tr>
<td>• Previous work experience</td>
<td>Student &amp; Employee Data</td>
<td>Student &amp; Employee Data</td>
<td>• Health status</td>
</tr>
<tr>
<td>• Dates of first and last employment</td>
<td>• Date of birth</td>
<td>• Date of birth</td>
<td>• Healthcare treatment</td>
</tr>
<tr>
<td>• Position number, type of appointment, service computation date, occupational group or class code, bargaining unit code</td>
<td>• Non-UH email address</td>
<td>• Non-UH email address</td>
<td>• Healthcare payment</td>
</tr>
<tr>
<td></td>
<td>• Job applicant records (names, transcripts, etc.)</td>
<td>• Job applicant records (names, transcripts, etc.)</td>
<td>Financial Aid Data</td>
</tr>
<tr>
<td></td>
<td>• Salary and payroll information</td>
<td>• Salary and payroll information</td>
<td>• FAFSA data</td>
</tr>
</tbody>
</table>
**Technical Guidelines**

http://www.hawaii.edu/infosec/techguidelines/

<table>
<thead>
<tr>
<th>Classification</th>
<th>Desktop/Workstation</th>
<th>Laptop/Notebook</th>
<th>Handheld Devices*</th>
<th>External Storage Drive*</th>
<th>Server*</th>
<th>Cloud Services*</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Sensitive</strong></td>
<td>Required</td>
<td>Required</td>
<td>Required</td>
<td>Required</td>
<td>Required</td>
<td>Required</td>
</tr>
<tr>
<td><strong>Restricted</strong></td>
<td>Required</td>
<td>Required</td>
<td>Required</td>
<td>Required</td>
<td>Required</td>
<td>Required</td>
</tr>
<tr>
<td><strong>Public</strong></td>
<td>Required</td>
<td>Required</td>
<td>Required</td>
<td>Required</td>
<td>Required</td>
<td>Required</td>
</tr>
<tr>
<td><strong>Semi-Sensitive</strong></td>
<td>Required</td>
<td>Required</td>
<td>Required</td>
<td>Required</td>
<td>Required</td>
<td>Required</td>
</tr>
<tr>
<td><strong>Site-Local</strong></td>
<td>Required</td>
<td>Required</td>
<td>Required</td>
<td>Required</td>
<td>Required</td>
<td>Required</td>
</tr>
<tr>
<td><strong>Exempt</strong></td>
<td>Required</td>
<td>Required</td>
<td>Required</td>
<td>Required</td>
<td>Required</td>
<td>Required</td>
</tr>
<tr>
<td><strong>External Use</strong></td>
<td>Required</td>
<td>Required</td>
<td>Required</td>
<td>Required</td>
<td>Required</td>
<td>Required</td>
</tr>
<tr>
<td><strong>Regulated</strong></td>
<td>Required</td>
<td>Required</td>
<td>Required</td>
<td>Required</td>
<td>Required</td>
<td>Required</td>
</tr>
</tbody>
</table>

*(Unless alternate approved security requirements/plans are filed with the UH Information Security Team)*

- **Device Registration**: Required
- **Physical Security**: Required
- **Logical Access Control**: Required
- **Anti-Virus**: Required
- **Firewall**: Required
- **File Storage Security**: Required
- **File Transmission Security**: n/a
- **Security Patch**: Required
- **Secure Configuration**: Recommended
- **Vulnerability Scanning**: Recommended
- **Vulnerability Remediation**: Recommended
- **Secure Remote Access**: Required
- **Logging**: Recommended
- **Single Purpose Use**: Recommended
### Key Regulations and Penalties (1)

<table>
<thead>
<tr>
<th>Regulation</th>
<th>Description</th>
<th>Penalty</th>
</tr>
</thead>
</table>
| **Family Educational Rights and Privacy Act (FERPA)** | • Federal law that protects the privacy of student education records  
• Access based on legitimate need to know  
• All student data are FERPA protected EXCEPT directory information  
• UH’s FERPA policy: AP7.022 | Potential loss of federal financial aid funding |
| **Higher Education Act (HEA)** | • Federal law that protects the federal financial aid information  
• Much more restrictive than FERPA | Potential loss of federal financial aid funding |
| **Gramm-Leach-Bliley Act (GLBA)** | • Federal law that requires financial institutions to explain how they share/protect customers’ data  
• Applies to higher ed because of financial aid  
• Recent addition: audit objective added to the Safeguards Rule | Financial fines, convictions |
<table>
<thead>
<tr>
<th>Regulation</th>
<th>Description</th>
<th>Penalty</th>
</tr>
</thead>
</table>
| Health Insurance Portability and Accountability Act (HIPAA) | Federal law that protects the privacy of health information  
• UH’s HIPAA policy: EP2.217 | Financial fines; breach notification to DHHS (and possibly state leg under HRS §487N) |
| General Data Protection Regulation (GDPR) | A European Union (EU) consumer protection law that applies to companies collecting PII as part of delivering goods and services  
• Regulation extends to colleges and universities  
• Applies ONLY when an individual is physically in the EU | Financial fines |
<p>| Payment Card Industry Data Security Standard (PCI-DSS) | A widely accepted set of policies / procedures that protects cardholders’ credit/debit/cash card transactions | Financial fines; breach notification under HRS §487N |</p>
<table>
<thead>
<tr>
<th>Regulation</th>
<th>Description</th>
<th>Penalty</th>
</tr>
</thead>
</table>
| Hawai‘i Revised Statutes (HRS) §487N | State law that defines the breach notification to the legislature  
• Written report to the legislature within 20 days after the discovery of a data breach  
• Data subject to regulation:  
  • FN or First Initial/LN combined with:  
    • Social Security Number (SSN)  
    • Driver license or state ID #  
    • Person’s financial account info (account #, access codes, passwords, etc.) | |

| Hawai‘i Revised Statute (HRS) Chapter 92F | State law also known as the Uniform Information Practices Act (UIPA) which requires open access to government records  
• Governs open records requests  
• Data subject to 92F-12:  
  • Employee data (e.g., name, salary range, bargaining unit, job title, business address/phone, employing agency, etc.) | Possible conviction |
### Key Regulations and Penalties (4)

<table>
<thead>
<tr>
<th>Regulation</th>
<th>Description</th>
<th>Penalty</th>
</tr>
</thead>
</table>
| National Institute of Standards and Technology Special Programs (NIST) 800-171 | • Federal Department of Defense (DoD) standards aimed at safeguarding Controlled Unclassified Information (CUI)  
• 110 controls in 14 areas (e.g., access, awareness and training, audits, incident response, risk assessment, etc.)  
• Expected to expand to financial aid data                                                                                                                            | Various criminal, civil, administrative, or contract penalties |
| National Industrial Security Program                                        | • DoD Directive 5220.22-M  
• National Industrial Security Program Operating Manual  
• Classified data subject to regulation                                                                                                                                                                                     |                                                   |
| Biological Safety Program                                                  | • Governs all research, teaching, and testing activities involving infectious agents and recombinant materials                                                                                                                 |                                                   |
| Export Control & International Traffic in Arms Regulations (ITAR)          | • Federal regulations that impose access, dissemination or participation restrictions on the use and/or transfer of commodities, technical data, or the provision of services subject to United States (US) export controls for reasons of national security, foreign policy, anti-terrorism or non-proliferation |                                                   |
Impact of Data Breaches / Exposures

- Loss of federal financial aid funding
- Financial fines
- Class action lawsuits
- Expenses, financial and human capital
- Loss of reputation / unfavorable publicity
- Additional legislative scrutiny
UH Data Related Policies and Procedures

**EP2.210**
Use and Management of Information Technology Resources

**EP2.211**
System and Campus Wide Electronic Channels for Communicating with Students

**EP2.212**
Data Classification Categories & Info Security Guidelines

**EP2.213**
Institutional Records Management and Electronic Approvals / Signatures (pending approval)

**EP2.214**
Institutional Data Governance

**EP2.215**
HIPAA (to be revised)

**EP2.216**
Online Approvals of Internal University Transactions

**EP2.217**
Student Online Data Protection Requirements (draft)

**EP2.218**
Policy on Contracts and Signing Authority

**EP2.219**
Mandatory Training & Continuing Education Requirements

**EP7.022**
FERPA
Purpose of Data Governance Process (DGP)
Formerly known as Data Sharing Request (DSR) Process

- **Inventory** where Protected Data is coming/goings
- **Protect**
  - Security – review how data will be collected, stored, and used
  - Legal – ensure agreements have appropriate language that protects UH
- **Communicate**
  - Share within and between campuses
  - Provide notice to our data and IT providers
- **Assess risk**
When the DGP is Required

Collecting, managing, sharing, exchanging, using and/or releasing Protected Data

- Can be internal or external to UH
- Can be for institutional or research purposes
- Includes personally identifiable and de-identified data
- Mainly applies to people data but can also include other non-people data that are sensitive in nature
Examples of Activities Involving Protected Data (1)

- Purchasing a product/services from a third party vendor (EP8.200)
  - Assessment software, tutoring services, texting services for potential students
- Releasing data to an external party
  - Cloud-based services
- Requesting a set of data that you normally do not have access to
  - Invite students with certain GPAs to join an honor society
- Establishing a continuous transmission of data from one source to another
  - Transfer student registration data to health services center to verify enrollment
- Connecting to the UH network
  - Use of UHM OneCard on vending machines, Pieology
Examples of Activities Involving Protected Data (2)

- Conducting research for a thesis/dissertation or other (requires IRB approval before submitting DGP)
  - A researcher wants grade data to evaluate his study on student cell phone addiction

- Storing non-UH data from a third party
  - Program doing a study for HIDOE, medical research project that downloads de-identified dataset from a databank

- Collecting data that is self-reported by individuals
  - Online form for employee parking requests, software for prospective students to apply and upload resumes/portfolios, HIDOE middle/high school students applying for TRIO and dual credit programs
Data Governance Process

Submit to DGO:
1. DGP form
https://datagov.intranet.hawi.edu/dgp/
2. Proposed agreement
3. IRB approval letter
4. Other supporting materials

DGO sends to Campus / System Executive Data Stewards

DGO Reviews
Clarify, resolve issues; revise draft contract language

VPIT Reviews / Approves

Program proceeds with signing agreement and data sharing

Procurement
No DGP But
VPIT Approval Required (EP8.200)

- Hardware and software purchases, $25k or more in aggregate
  - Servers, desktop computers, laptops, printers, smart TVs, and other types of electronic equipment that will be connected to a University network
- Software (shrink-wrapped or “click-through” T&Cs)
- https://www.hawaii.edu/its/support-tools/
Language in Lieu of an Indemnity Obligation
(EP8.200, Appendix 12-e)

“The University shall be responsible for damage or injury caused by the University's officers and employees in the course of their employment to the extent that the University’s liability for such damage or injury has been determined by a court or otherwise agreed to by the University….. The [Name of other contracting party] acknowledges that this provision, in itself, shall not constitute or be interpreted to be any type of indemnification, defense, or hold harmless obligation of the University. The University’s obligations under this Section shall survive the expiration or earlier termination of this Agreement.”
OVPIT/CIO PROCUREMENT APPROVAL REQUESTS

- Request OVPIT approval for non-compliant terms (shrinkwrap terms) waiver
- List view of all pending and completed requests for non-compliant (shrinkwrap terms) waiver
- Request OVPIT approval for IT procurement
- List view of all pending and completed requests for IT procurement
Small purchases; shrink-wrapped or "click-through"

Small purchase non-standard terms request (for VP IT/CIO approval)

This form is used to submit requests for approval of non-standard contract terms under small purchase transactions (p-card), where traditional "shrink-wrap" terms do not provide for modification by the vendor, and are also typically click-to-accept during the purchase process. Any questions regarding the process or variations from standard contracting practices should be referred to your FA, OPM or OGC.

Larger purchases, including those requiring an actual signature by the vendor (that implies the opportunity for modification of terms) are generally NOT eligible for review under this process. Such requests may be returned for clarification, or denied unless additional rationalization is provided with the request.

Requests submitted via this form will be routed to OVPIT for review and approval. Requestor will be provided notification of approval or denial of request; the completed request will remain archived online for future reference. Requestors shall attach any applicable documentation, including terms with non-standard or otherwise offensive language.
IT Purchases $25,000 or more

IT procurement request OVPIT/CIO approval

This form is used to submit requests for approval IN ADVANCE of any IT procurement that exceeds $25,000, OR if the product or service to be procured requires integration with ANY ITS managed system (inclusive of ID management, enterprise systems and ITS developed and maintained localized applications).

Approval is REQUIRED prior to contract/PO execution - NOTE: integration requirements should be resolved PRIOR to any contracting effort, preferably as early as possible in the procurement process. Any questions regarding the process or variations from standard contracting practices should be referred to your FA, OPM or OGC.

Requests submitted via this form will be routed to OVPIT for review and approval. Requestor will be provided notification of approval or denial of request; the completed request will remain archived online for future reference. Requestors shall attach any applicable documentation.
To Summarize

- Requires DGP
  - Transfers of Protected Data
  - May include purchases of products and/or services
  - [https://datagov.intranet.hawaii.edu/dgp](https://datagov.intranet.hawaii.edu/dgp)

- Requires VPIT approval
  - No Protected Data involved
  - Hardware and software purchases of $25K or more
  - Software (shrink-wrapped or “click-through”)
  - [https://www.hawaii.edu/its/support-tools](https://www.hawaii.edu/its/support-tools)
Data Governance
Principles and Guidelines (1)

- Access to Protected Data will be based on a need-to-know
- Minimal access will be granted whenever possible
  - i.e., the most restrictive set of permissions and privileges will be granted, and only for the duration needed
- De-identified data will be provided whenever possible
- Duplication of data is discouraged
- Data requested for a specific purpose cannot be used for another purpose, i.e., re-purposed and re-disclosed
Data Governance Principles and Guidelines (2)

- Data within a record or document will be protected based on the data element with the highest level of sensitivity.
- Be aware that a data element may not be personally identifiable, but when combined with other data elements, it may become personally identifiable.
- Be aware of small cell sizes in reports.
- When accessing data outside of work, do not use unprotected or public wireless connections.
- When data is no longer needed—redact, remove, or destroy it!
Information Security Update

Jodi Ito, Chief Information Security Officer (CISO)
Security & Privacy Outweigh Convenience!
IT’S ALL ABOUT THE DATA!!

- What data elements are involved?
  - E.g. full name, date of birth, SSN, home address, medical treatment info, etc.

- Is the data UH Protected Data?
  - E.g. restricted, Sensitive, Regulated, HIPAA, PCI, CUI, ITAR, GLBA, etc.

- Is it being protected in accordance with UH policies and procedures?
  - If a 3rd party vendor is involved, has appropriate contract language or terms & conditions been signed/approved?

- How much data is involved?

- How long is the data retained?

- What **authorized** business purpose is involved?
Federal Concerns About Academic Research

- “Dear Colleague” letters about protection of information
  - http://www.ors.hawaii.edu/

- FBI report:

- Cybersecurity Maturity Matrix Certification (CMMC)
  - Requirements released Jan. 2020
  - ”contractor” must certified by 3rd party assessor; Ranked against 5 levels; if not certified at appropriate level of contract/agreement, will NOT receive the contract/award
Other Indicators of Concern

- A-133 Audit
  - Universities being audited against GLBA for the first time
- More alerts from federal agencies & ISACs
  - Compromised UH systems
  - Compromised UH accounts
- Expecting update to HRS 487N – task force convened to expand data elements & look at privacy issues
What’s wrong with this email?

“Display name” shows “University of Hawaii System” but email address is “automated-message@everfi.net”

Poor grammar

Suspicious link:
https://notifi.fifoundry.net/tracks/b7848a06-3d08-4ed0-a46d-98c9902e7e90/click/BAh
What’s wrong – continued:

Always be cautious about entering your UH username and password – verify the site is legitimate.

Since email itself is suspicious, you should also be cautious about clicking on links in the suspicious email.

If you have difficulty logging in, check out the technical info at the bottom of this page.

Technical Info:

- Log in with your UH username and password. If you were directed by the department to take the training and do not have a UH username and password, create a username and password on the login page.
- Work at your own pace from any computer or tablet
- Courses will save your progress if you need to stop and return later
- Courses are best supported by the latest versions of Chrome, Firefox, and Safari (preferred), or Microsoft Internet Explorer 11+
- Need more help? Contact EVERFI’s 24/7 tech support using “Help” within the course or by visiting support.everfi.com
Recent Examples of Data Mishandling

- UH 3rd party web application exposed personally-identifiable information such as first name, last name, birthdate, gender:

```javascript
r.eComplete='';r.appdate='201909171';r.device='';
r.r.setInitialValues( {"fname":"xxxxxxx","lname":"xxxxxxxxxx","email":"xxxxx@yyyy.zzzzzz","gender":"x","mname":"x","country_cd":"USA","pname":"xxxxxxx","birth_day":"xx","birth_month":"xx","birth_year":"xxxx"} );r.cjSettings = [];
r.uExported=false;r.securityLevel=3;
```
More Examples of Data Mishandling

- Application developer required **FULL SSN + Date of Birth** for authentication
- 3rd party vendor stored **personally identifiable information UNENCRYPTED** in their development environment and the system was compromised
- 3rd party vendor website is “requiring” use of UH username and password as the login credentials BUT is NOT using the UH authentication process (vendor is storing UH username and password)
Requiring Use of UH Credentials for non-UH applications
Chegg, a technology giant specializing in textbook rental, has confirmed a data breach affecting some 40 million customers.

In a filing with the Securities and Exchange Commission, the company said it will reset all user passwords after hackers gained access to the company’s customer database. That database includes users for Chegg’s website but also other products, such as citation service EasyBib, which it owns.

The breach occurred in April, but was only discovered a week ago.

Hackers stole usernames, email addresses, shipping addresses and hashed passwords, the company said, but doesn’t believe that financial data was taken.

The company went public in 2013, and is currently worth $3.3 billion. Chegg’s stock is down more than 10 percent a day after the breach was revealed.

Chegg Impact to UH

- Over 10,000 UH accounts identified
- Over 1000 accounts used the same UH password and were disabled
- Accounts were being used by the attackers to send spam; could have been used for other malicious purposes
- Increase in “man-in-the-middle” email attacks
Email "man-in-the-middle" attack

- Attacker has the password for the email account
- Attacker reads everything in the mailbox
- Attacker selectively replies to emails impersonating the actual user and deletes the replies from the “sent” mail folder
- Used to conduct financial fraud
  - Re-directing payments, payroll, etc.
Information Security Program

- The University of Hawai‘i Information Security Program is comprised of the following strategic areas:
  - Data Governance and Oversight
  - Information Security Audits & Risk Assessments
  - Information Security Policies & Procedures
  - Identity Management & Access Controls
  - Information Security Training and Awareness

- http://www.hawaii.edu/infosec/infosecprogram/
Regulations & Compliance

- Payment Card Industry Data Security Standards (PCI-DSS)
  - Collecting credit card payments?

- Health Insurance Portability and Accountability Act (HIPAA)
  - Using medical data? Providing medical treatment? And more…

- Controlled Unclassified Information (CUI – NIST 800-171)
  - Government contracts? Prime or sub-contractor with DFARS 252 clause specified in the contract?

- Family Education Rights and Privacy Act (FERPA)
  - Student data?

- GLBA – UH being audited against GLBA this year (new!)
  - Collecting/distributing payments on behalf of an individual? E.g. student financial aid, One Card
Protect Your Data!
Protect Your Accounts!
Protect Your Computers!
YOU ARE A TARGET!
Protect Your Data!

- Know which files have sensitive information
  - Use Spirion (formerly Identity Finder) to scan for sensitive information
  - [http://www.hawaii.edu/askus/1297](http://www.hawaii.edu/askus/1297)

- Protect sensitive/regulated data as required by UH policy

- Back up your data regularly and protect sensitive/regulated information by encrypting the sensitive/regulated data
Protect Your Data - continued

- Securely delete any sensitive information that is not needed anymore
  - Don’t keep sensitive data “just in case”

- Physically secure/protect any repositories of sensitive information
  - Paper documents stored in secured locations, not accessible by unauthorized individuals
  - External hard drives with sensitive information should be stored in secured locations (locked file cabinets, etc.)
Do **NOT** store sensitive or regulated information in Google Docs or on Google Drive!
UH Number vs. SSN

- UH Number is a unique identifier for each person affiliated with UH
- Intended to replace SSN with a safe alternative
- Classified as “Restricted”
  - Should NOT be able to access PII or other sensitive information with only a UH number
Protect Your Account!

- Compromised UH accounts are being used by attackers for:
  - Launching phishing & spamming campaigns
  - Committing financial fraud (Business Email Compromises)
- Use Multi Factor Authentication (Duo)
  - [https://www.hawaii.edu/askus/1758](https://www.hawaii.edu/askus/1758) (set up)
- **IS REQUIRED** for Hawaii Information Portal (HIP)
  - [https://www.hawaii.edu/ohr/new-payroll-system-will-require-your-action/](https://www.hawaii.edu/ohr/new-payroll-system-will-require-your-action/)
Multi Factor Authentication at UH - DUO
http://www.hawaii.edu/its/uhlogin/
Protect Your Account!

- Use strong passwords & a strong password management strategy
  - DO NOT RE-USE PASSWORDS!
  - Use hard to guess passwords; no dictionary words, include upper/lowercase, numbers AND special characters
  - Ex: bL00&Kuki@0712 (favorite color blue, favorite food cookie, MMDD password was created)
- Check your password strength: https://lastpass.com/howsecure.php
- Change passwords regularly

- Monitor your accounts for suspicious activity
Check Your UH Account

- From the UH web Gmail page, after logging-in, click on “Details” on the bottom right of your screen:
Activity Window

- Check “Date/Time”
- Check ”Access Type”
Protect Your Computers!

- Apply operating system and application updates frequently and regularly
- Install and update protective software such as anti-virus software
- Back up your data regularly and protect sensitive/regulated information by **encrypting** the sensitive/regulated data
- Never leave your devices logged-in & unattended; control access to your machines
Protect Your Data!

Protect Your Accounts!

Protect Your Computers!

YOU ARE A TARGET!
Top 10 Cyber Security Practices

1. Recognize that YOU, YOUR DEVICES, and YOUR INFORMATION are targets; know the threats

2. Practice good password management;
   a. Use multi-factor authentication (Duo at UH)
   b. Use STRONG passwords

3. Apply operating system and application updates frequently and regularly

4. Install and update protective software such as anti-virus software

5. Back up your data regularly and protect sensitive/regulated information by encrypting the sensitive/regulated data
6. Use a secure network for sensitive transactions (not the coffee shop wi-fi or hotel computer)

7. Never leave your devices logged-in & unattended; control access to your machines

8. Use email & the Internet safely; be careful when clicking on attachments or links in email

9. Monitor your accounts for suspicious activity

10. Be careful what you share online & on social media (know your digital footprint)
Web Accessibility and Compliance

Mitchell Ochi
Director, ITS-Client Service and Operations Center
The Law

- **Section 504 of the Rehabilitation Act of 1973**
  Prohibits discrimination on basis of disability in programs/activities receiving federal financial assistance

- **Title II of the Americans with Disabilities Act of 1990**
  Prohibits discrimination on basis of disability by public entities

- **Section 508 of the Rehabilitation Act of 1973**
  Requires equal access to information for disabled users and non-disabled users, and provides accessibility standards and requirements for information technology
Guidelines and Techniques

- Web Content Accessibility Guidelines (WCAG)
  WCAG 2.0 - https://www.w3.org/TR/WCAG20/
  WCAG 2.1 - https://www.w3.org/TR/WCAG21/

- Web Accessibility Initiative - Accessible Rich Internet Applications (WAI-ARIA) 1.0
  https://www.w3.org/TR/wai-aria/
Who is responsible?

- Anyone who owns or manages content on the Web

Content includes
- Web pages
- PDFs
- Microsoft Office (Word, Excel, Powerpoint) documents
- Videos

- Section 508 specifies content must meet WCAG 2.0 Level A and AA guidelines for accessibility compliance
Why is this important?

- “Commitment to Access” part of UH EP 2.210
- UH is under a Voluntary Resolution Agreement (VRA)
  VRA text -
  https://www.hawaii.edu/access/resources/uhvra/
Plan for New Content

- Plan for New Content has been sent to the Office of Civil Rights (OCR)
- Plan posted online
  [https://www.hawaii.edu/access/resources/uh-content-plan/](https://www.hawaii.edu/access/resources/uh-content-plan/)
- “Living” document
What is ITS doing?

- **Tools**
  - Website accessibility scanning
    - Siteimprove (PDF scanning as well)
    - SortSite
  - Adobe Acrobat Pro DC (all faculty and staff)
  - Grackle Suite (all Google@UH accounts)
  - Augusta ADA Solution for video transcription/captioning (all faculty and staff)
What is ITS doing? (cont’d)

- Annual reports of website accessibility

- Training
  - Online Accessibility Training
    - LinkedIn Learning (formerly Lynda.com)
    - Siteimprove Academy
    - Other online training resources
  - Opportunistic in-person training
What can I do?

- Assess site inventory
  - Is there content that can be retired/removed?

- Check accessibility of current content
  - Setup your site to be scanned by Siteimprove
    * Login-protected sites with protected data - use SortSite or the Siteimprove Chrome plug-in
  - Be thoughtful and plan for any remediation effort
  - Prioritize content remediation
What can I do? (cont’d)

- Sign up for free training accounts
  - LinkedIn Learning - [https://www.hawaii.edu/sitelic/lynda/](https://www.hawaii.edu/sitelic/lynda/)
  - Siteimprove Academy - email [itsada@hawaii.edu](mailto:itsada@hawaii.edu)

- Get your Adobe Acrobat DC license
  [https://www.hawaii.edu/sitelic/adobe/](https://www.hawaii.edu/sitelic/adobe/)

- Check for updates on VRA-related activity - [https://www.hawaii.edu/access/resources/vra/](https://www.hawaii.edu/access/resources/vra/)
Need Help?

- Accessibility questions - itsada@hawaii.edu
  UH Accessibility Website - https://www.hawaii.edu/access

- IT questions, off-hours help
  ITS Help Desk (24x7 availability)
  (808) 956-8883, (800) 558-2669 [toll-free]
  help@hawaii.edu
Today’s presentation slides and Fall 2019 schedule

https://datagov.intranet.hawaii.edu/training/

Please give us your feedback!

http://go.hawaii.edu/gzG
Questions?

Sandra Furuto, Data Governance Director, yano@hawaii.edu
Jodi Ito, Chief Information Security Officer, jodi@hawaii.edu
Mitchell Ochi, Client Service & Operations Center Director, ochi@hawaii.edu