The University of Texas Rio Grande Valley™

Information Security Office

Francisco Tamez
Security Analyst

www.utrgv.edu/is ESRAX 1.110 is@utrgv.edu

Policy Reviews

TAC 202

- Stablish information Security Standards for Institutions of Higher Education
- States the rules for: Responsibilities of the Institution Head, Information Security Officer, and Staff.

UTS 165

- It is the policy of The UT System to protect Information Resources based on Risk against accidental or unauthorized access, disclosure, modification, or destruction and assure the availability, confidentiality, and integrity of these resources.

UTRGV AUP

- Acceptable Use Policy for users and computers accessing UTRGV information resources as defined by UTS 165

Information Resources Acceptable Use and Security Policy (AUP)

- Users have no expectation of privacy regarding any data residing on university owned computers, servers, or other information resources owned by, or held on behalf, of university.

- Users have no expectation of privacy regarding any University Data residing on personally owned devices.

- Use of University Information Resources to intentionally access, create, store, or transmit sexually explicit materials is prohibited unless such use is required as part of the User's official duties as an employee of University and is approved in writing by the President or a specific designee.

Information Resources Acceptable Use and Security Policy (AUP)

- Users shall store Confidential Information or other information essential to the mission of University on a centrally managed server, rather than a local hard drive or portable device.
- In cases when a User must create or store Confidential or essential University Data on a local hard drive or a portable device such as a laptop computer, tablet computer, or, smart phone, the User must ensure the data is encrypted in accordance with University System's and any other applicable requirements.

- Users who store University Data in the cloud must use services provided or sanctioned by the University, rather than personally obtained cloud services.

Information Resources Acceptable Use and Security Policy (AUP)

- Users are to use University provided email accounts, rather than personal email accounts, for conducting University business.

- University issued or required passwords, including digital certificate passwords, Personal Identification Numbers (PIN), Digital Certificates, Security Tokens (i.e. Smartcard), or similar information or devices used for identification and authorization purposes shall be maintained securely and shall not be shared or disclosed to anyone.

UTRGV

ActiveSync Policies Changes for Personally Owned Mobile Devices (BYOD) connecting to your UTRGV email

If you have configured your personal mobile device to read your UTRGV email through Exchange (Office 365), basic security settings will be enforced and applied by ActiveSync to protect stored data from unauthorized access should your mobile device be lost or stolen.

Effective May 31, 2017

UTRGV

ActiveSync Policies Changes for Personally Owned Mobile Devices (BYOD) connecting to your UTRGV email

The following four policies will now be enforced and applied by ActiveSync:

1. Your mobile device will need to be encrypted.
2. All devices connecting to the University Exchange system (Office 365) will be required to have a five-digit PIN/Passcode.
3. Your device's screen will lock after five minutes of **inactivity**, you will have to re-enter your PIN/Passcode to resume using your mobile device.

NEW!

UTRGV

ActiveSync Policies Changes for Personally Owned Mobile Devices (BYOD) connecting to your UTRGV email

If you do not wish for these controls to be implemented on your personal mobile device, simply **remove** your University email account from the mobile device.

If you need assistance with or are having problems with your mobile device configuration, please contact the IT Service Desk. Better assistance can be provided for mobile device issues in person.

IT Service Desk:
Edinburg, EACSB 1.112 (next to the ID card office)
Brownsville, BMAIN 1.212A (next to uCentral, tower at Main)

(956) 665-2020 or (956) 882-2020

Report a Security Incident

Information Security Office
www.utrgv.edu/is

Police Department
www.utrgv.edu/police

Security Incident

Lost/Theft of computing device

- Computer, Laptop, Tablet
- All University owned computing devices and Personal (used for storing University data)

Lost/Theft of electronic storage device

- Thumb drive, USB, DVD, CD, etc.

Unauthorized or Unintended disclosure of Confidential or Sensitive information

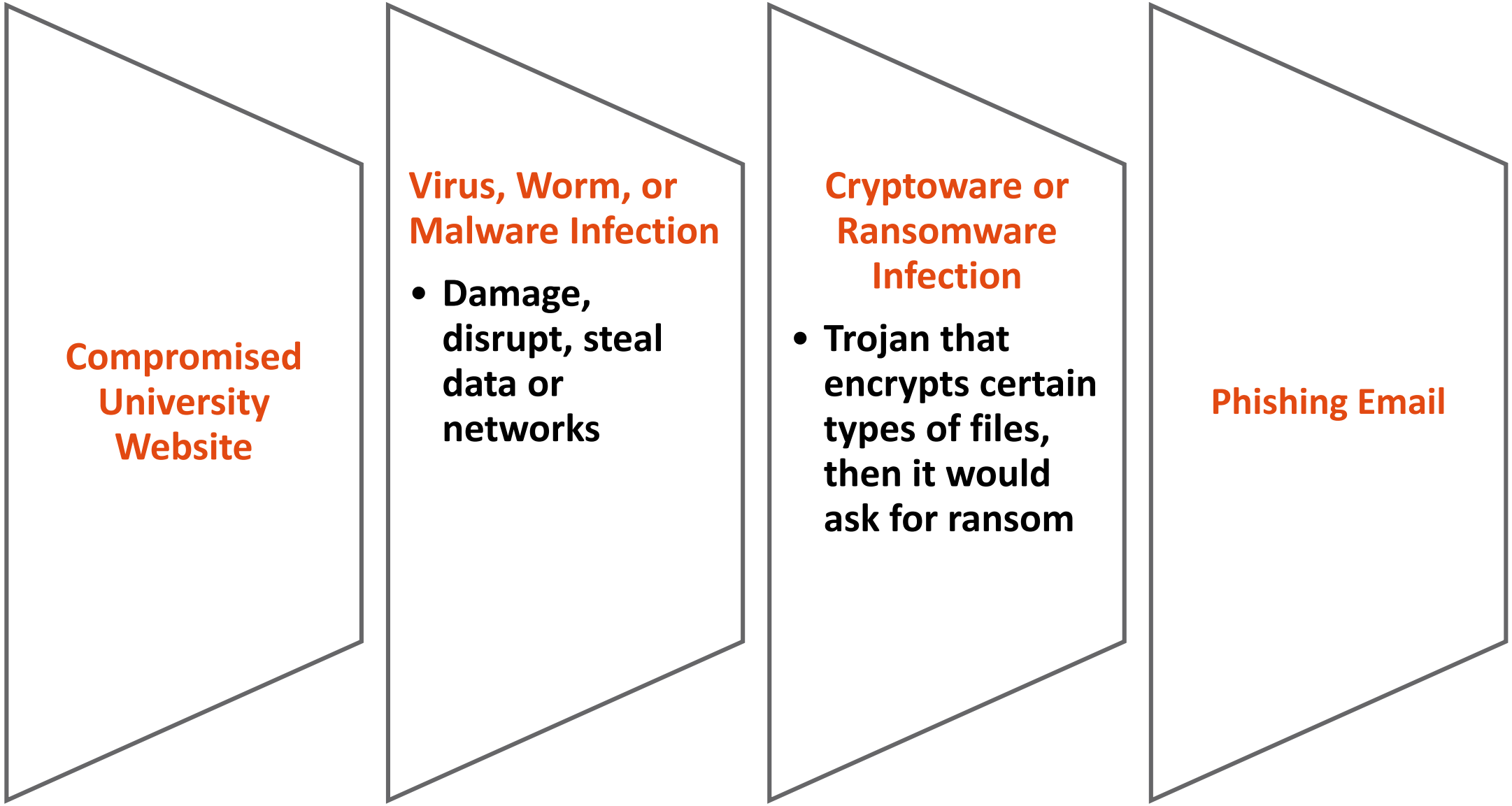
- Credit Card Number
- SSN

Compromised Credentials

- UTRGV accounts and password

Cyberstalking, Bullying, or Harassment

Security Incident Cont'd



IRS

Department of the Treasury
Internal Revenue Service

05/18/2016

Reference: I3H583326/16

Claim your Tax Refund Online

Dear Taxpayer,

We identified an error in the calculation of your tax from the last payment, amounting to $319.95.

In order for us to return the excess payment you need to create a e-refund account after which the funds will be credited to your specified bank account.

Please click “Get Started” below to claim your refund:

Get Started

viruswebsite.net/inc/.s/

From: University of Memphis Webmail Management [webmaster@memphis.edu]

Sent: Thursday, May 19 2016 3:52 PM

Subject: VERIFY YOUR EMAIL ACCOUNT

Attention Outlook Web User

This message is to all University of Memphis Webmail Users

We are currently upgrading our data base and webmail network.

All inactive email accounts will be deleted, as we intend to create more space for registration of new users (Staff and Students).

To prevent your account from being deleted, we kindly request that you confirm your account information for update, by providing the information below.

Username:
Password:

Warning! Failure to o this will render your email permanently.

Thanks for your understanding

Warning Code: VX2G99AAJ

University of Memphis Webmail Management

From: Mafenya, Nkhangweleni [mailto:mafennp@unisa.ac.za]

Sent: February-19-16 11:12AM

Subject: Faculty & Staff Notification

This message (and attachements) is subject to restrictions and a disclaimer. Please refer to http://unisa.ac.za/disclaimer for full details

Dear Faculty Staff & Employee Email Subscribers

Welcome to 2016 Academic Session

Your Email Account have been put on-hold by our server, you can no longer send or receive emails, to avoid this kindly click on the link IT HELPDESK to submit your old account for New to enable you to send and receive emails.

Thank You

http://notifications pandaform.com/pub/ujw35t/new

Report Phishing

If you receive an email that you suspect may be a phishing message:

Forward email to itdns@utrgv.edu

www.utrgv.edu/it/how-to/report-phishing-messages

Data Management

- Standards
- Data ownership
- Data classifications
- Identity Finder
- Retention Schedules
- Where can I store University Data?

Standards that protect

Data Management

- ✓ Standards
- Data ownership
- Data classifications
- Identity Finder
- Retention Schedules
- Where can I store University Data?

Data Ownership

- Individual with the responsibility of carrying out the program that uses the resources

For example

- Are you a principal investigator for a research project?
- Are you an administrator in charge of a business function?
- Are you a faculty member who maintains a grade book?
- Do you have one of the following titles: Dean, Chairman, Director, Manager, Coordinator, etc.

Data Owner Responsibilities

- Approving access to information resources and periodically review access lists based on documented risk management decisions;
- Formally assigning custody of information or an information resource;
- Coordinating data security control requirements with the ISO;
- Classifying information under their authority, with the concurrence of the state institution of higher education head or his or her designated representative(s), in accordance with institution of higher education's established information classification categories;

Data Management

- ✓ Standards
- ✓ Data ownership
- Data classifications
- Identity Finder
- Retention Schedules
- Where can I store University Data?

C.I.A.

Confidentiality

Integrity

Availability

One of the primary goals for the ISO is to ensure the C.I.A of data

DATA CLASSIFICATION	DESCRIPTION	EXAMPLES
CONFIDENTIAL (CATEGORY I)	Information (or Data) is classified as **Confidential** if it must be protected from unauthorized disclosure or public release based on State or Federal law or regulation, and by applicable legal agreement to the extent permitted by law.	• A social security number • Student education records subject to FERPA. • Patient billing Information and Protected Health Information subject to HIPAA or applicable state law.
CONTROLLED (CATEGORY II)	The **Controlled** classification applies to Information/Data that is not generally created for or made available for public consumption, but may be subject to release to the public through request via the Texas Public Information Act or similar State or Federal law.	• Operational records, operational statistics, employee salaries, budgets, expenditures. Internal communications that do not contain Confidential Information. • Research Data that has not yet been published, but which does not contain Confidential Information protected by law.
PUBLISHED (CATEGORY III)	**Published** Information (or Data) includes all Data made available to the public through posting to public websites, distribution through Email, Social Media, print publications, or other Media.	• Statistical reports, Fast Facts, Published Research, unrestricted directory Information, educational content available to the public at no cost.

Why data needs to be protected?

Personally Identifiable Information (PII)

Type: Data that uniquely identifies a person (SSN, DOB, Credit Card, Name, Address)

Who wants it: Identity thieves

Reason: Financial gain, to commit fraud

Intellectual Property (IP)

Type: Research, Inventions, literary and artistic works, design, images

Who wants it: Competitors, opportunists

Reason: Personal credit, patents, technological advance, financial gain

How does C.I.A play a part in this?

Data Management

Standards

Data ownership

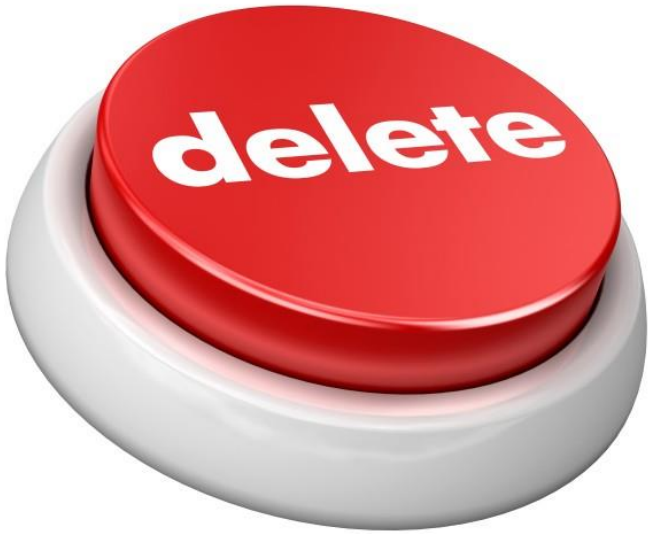
Data classifications

Identity Finder

Retention Schedules

Where can I store University Data?

Delete



&

Shred

Identity Finder

Will allow you to:

a. Secure or delete (Shred) digital files

- Delete the files for PERMANENT disposal
- Encrypt and password protect the files, if you MUST have them on your computer

b. Find files in your computer that contain protected data

- SSN, Credit Card Number, Password

c. Should be pre-install on all University owned computers.

- If not, contact the IT Help Desk

identityfinder

www.identityfinder.com

Retention Schedules

Is used to authorize requests for destruction of records.

Example:

Record Series Title	Retention Period
Transcripts from High School	AC +5
Origin foreign Transcripts enrolled or not enrolled	PM
HIPAA (Health Insurance Portability and Accountability Act) Related Documentation	AC +6
Transfer or Budget Revisions	FE+3

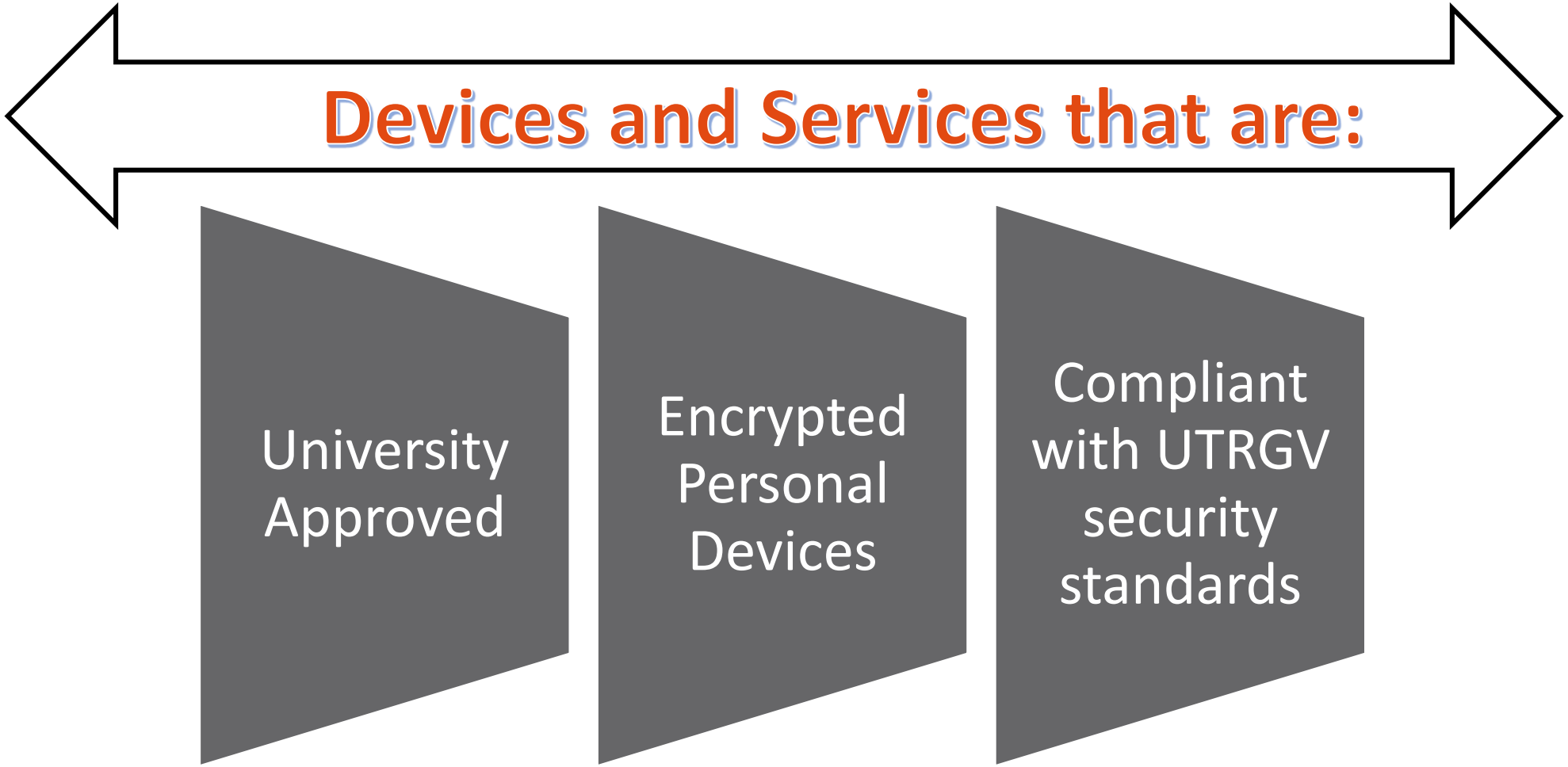
Contact Records Management Services (RMS) recordsmanagement@utrgv.edu for any questions concerning retention codes.

AC – After Closed, Terminated, Completed, Expired, Settled

FE – Fiscal Year End

Data Management

Where can I Store University Data



Data Management

So How do we protect data at rest?

Encrypt

Transformation of data into a form that conceals the data's original meaning to prevent it from being known or used.

Encryption is especially important if you are trying to send sensitive information that other people should not be able to access.

To properly encrypt sensitive digital files you can use identity finder.

Remember that encryption does not protects you from virus/malware it protects you from unintended disclosure due to loss or theft.

Protect data in motion

Because email messages are sent over the internet and might be intercepted by an attacker, it is important to add an additional layer of security to sensitive information.

To send an encrypted email just include [secure] at the beginning of the subject field of your email.

Example:

Subject: [secure] Monthly Report

www.utrgv.edu/it/how-to/email-encrypt-decrypt

Approved Storage Devices
Transport Media

APRICORN

Computers connecting to Information Resources

Requirements

- Required Configuration and Security Software
- OS & OS patches have to be installed expediently

Data Backups

- Your responsibility
- Only to approved sources

Where to get help with University owned computer problems

- IT Service Desk (665-2020 or 882-2020)

UTRGV iShop

Get I.T.

BEFORE YOU

Passwords

Why are passwords important?

- They provide validation
- They allow access and authorization
- They protect our data/information

Your UTRGV password allows access to

- Email
- Student records (FERPA) – subject to role
- Network access (Wired and WiFi)
- Confidential Files / Research papers (IP)
- Employee Data (Your SSN, Direct Deposit, Contact Info, Home Address)

Passwords (Cont'd)

Password Requirements

The 5 Mandatory Password Guidelines

1. **You Shall Choose One Wisely**

   Password123 VS #eY7453AB!! VS MyPassphraseRocks2!

2. **You Will Never Write It Down**

   NEVER!

3. **You Will Never Share It With Anyone**

   Not even your supervisor, IT, or Security (ISO)

   UTRGV personnel will never ask for it

4. **You Can Change It Often**

   At least once per year (per policy)

5. **You Will Be Mindful of Where You Use It!**

   Be careful of fake websites that are made to look real

Multi Factor

Multi Factor Authentication

1. Something you know (e.g. passphrase)
2. Something you have (e.g. bank card, mobile phone, token)
3. Something you are(Biometrics: Fingerprint, voice, retina)

UTRGV™ Uses DUO-Security for two factor authentication when accessing secure sites or establishing a VPN connection to the campus

http://www.utrgv.edu/it/how-to

Reminder

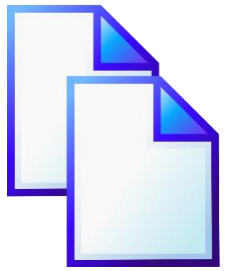
Policy violation to use UTRGV passwords in none UTRGV systems.

- Facebook
- Gmail
- Twitter
- This also includes 3rd party services in use by UTRGV but that are not maintained by UTRGV (e.g. IRBNet)

Feedback: bit.ly/UTRGVISONEOF

The University of Texas Rio Grande Valley™

Information Security Office



www.utrgv.edu/is

www.facebook.com/UTRGVISO

The University of Texas Rio Grande Valley™

Information Security Office

Francisco Tamez
Security Analyst

www.utrgv.edu/is ESRAX 1.110 is@utrgv.edu