UTRGV ISO NEWSLETTER

www.utrgv.edu/is

The University of Texas Rio Grande Valley™

Information Security Office

VOLUME I, ISSUE V MAY 10, 2017

INSIDE THIS ISSUE:



EDITOR

Francisco Tamez

*ISO Security Analyst*

# Spring Cleaning

In Spring we celebrate the renewal of life, ideas of rebirth, regrowth that occurs in nature, and eagerly await the exciting fun of summer. By tradition, spring cleaning means cleaning, dusting, and mopping; for this issue the Information Security Office (ISO) invites you to consider taking a few minutes to spring clean your digital life.

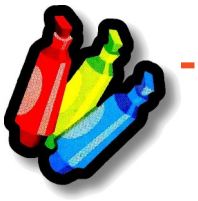
Please follow these tips that will guide you to refresh and renew your cyber life, and remember to share them with your friends and family.

**Clean your digital accounts:**

- Online — Online accounts collect clutter and require a couple of minutes to clean. Go through your accounts for both work and home (e.g., email, social networks, clubs, shopping, and cloud storage). Go through their information and ask yourself if there is information in those accounts that you don't need anymore, such as credit cards saved in your accounts, or perhaps there are accounts that you don't use and can close.
- Email — There may be information in your accounts that you can archive into folders or delete. A great idea is to set rules, by using rules you can reduce manual and repetitive actions, these can help you to stay organized that will automatically move messages (e.g. spam), empty your deleted items or trash folder on a regular basis.
- Social Media — Spring clean your social media accounts by following our "Don't get **SMACK**ed" campaign. Review the privacy and security settings on websites you use to ensure they're at your comfort level for sharing. It's OK to limit how and with whom you share information.

**Clean your devices:**

- Smartphones, tablets, laptops, and computers require maintenance and spring cleaning is the perfect chance to do it! Delete unused applications or software and clear out any downloads you aren't using any more. Check for old files that can be archived or deleted. Make sure your device's security software is working properly and all software is patched and set to auto-update.
- Last, but not least, take out the trash. Literally. There may be old devices in your house or office that could be recycled. All UTRGV computer hard drives must be removed and sanitized to ensure that any sensitive or confidential information it may contain is permanently erased and unrecoverable before the computer can be sent to surplus. The ISO strongly recommends an identical course of action for personal devices.



# SECURITY HIGHLIGHTS

**Update alternate email address and security questions for UTRGV account self-service website**

Update the alternate email address linked to myaccount.utrgv.edu to a personal account (Yahoo, Google, etc.). This will ensure that you can continue to utilize important account recovery features such as:

- Request a password reset link
- Request an account unlock link
- Request a forgotten username

To learn **how to** Update your Alternate Email Address please visit: www.utrgv.edu/it/how-to/account-management-update-alternate-email-address

Additionally, update the security questions associated with myaccount.utrgv.edu to ensure the availability of all account recovery options.

To learn **how to** Update your Security Questions please visit: http://www.utrgv.edu/it/how-to/account-management-update-security-questions/index.htm

**Information NOW available**

The Information Security Office (ISO) has released new standards and guidelines. These were written to ensure compliance with Federal, State, and UT System requirements. Using a model of "trust but verify", these standards can be audited to validate compliance:

- Data Classification Standard
- Data Classification Guide
- Minimum Security Standards for Data Stewardship
- Extended list of Confidential Data

For more policies and standards feel free to visit our website: www.utrgv.edu/is/en-us/resources/policies-tabs/

**Leaving for vacation?**
If you are planning on your spring vacation and you will not be using your office computer, then don't forget to turn it off. By leaving your computer off you are protecting your information and you are saving energy at the same time!

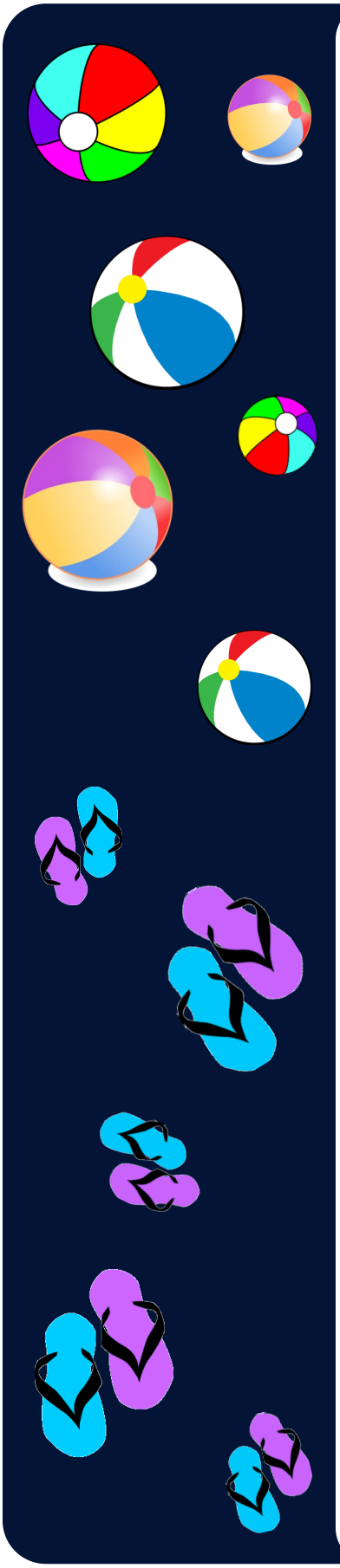
**Millions of college credentials spotted on dark web**

Researchers have found 13,930,176 email addresses and passwords belonging to faculty, staff, students and alumni of major universities across the country on the dark web.

The University of Michigan topped the list of higher education institutions with the most credentials on the dark web with 122,556 accounts, followed by a host of other Big 10 universities including Ohio State, University of Nebraska, Pennsylvania State University, University of Minnesota, and University of Illinois at Urbana-Champaign, according to a recent report published by Digital Citizen's Alliance.

Researchers said that when broken down by state, the largest number of credentials posted came from schools in California, followed by New York, Michigan, Texas, and Pennsylvania which are all among the top 10 most populous states. "Stolen credentials can be the first step down the path to more sensitive personal information, access to valuable intellectual property, and potentially identity theft," researchers said in the report, adding that some individuals may have been driven by revenge or just mayhem and destruction.

bit.ly/millionsofcollegecredentials



# End Of Life Software

**EOL Software**
Software applications have a lifecycle. The lifecycle begins when the software is released and ends when it is no longer supported by the vendor, also called End Of Life (EOL). When software stops being supported by the vendor it can lead to no longer receiving security updates that can help protect your PC from harmful viruses, spyware, and other malicious software that can steal your personal information.

**EOL OS**
Windows XP and Apple OSX 10.8 and below are EOL. If you are currently using an EOL Operating System (OS) you should upgrade your OS to maintain the security of your computer and data. Computers owned, leased or managed by UTRGV must adhere to the Computer Security Standard, (bit.ly/UTRUTRGVISOComputerSecurityStandard) which requires them to run only vendor supported OS.

**Today's EOL products**

| Product | Version | Product | Version |
|---|---|---|---|
| Windows | Vista | Adobe Acrobat | 9.x |
| Windows | 8.0 | Adobe Flash Media | 4.5 |
| Adobe Acrobat X | 10 | Adobe Flash Player | 19 |
| Adobe Reader | 9.x | Java SE | 7 |
| | | QuickTime for Windows | |

To successfully update to the latest OS you will need the following systems requirements. In the instance that the computer's hardware is not capable to stand the latest OS, then according to the computer security standard that computer will have to go through surplus and a new one with capable hardware will take its place.

If you use for your work activities a university owned computer with an Operating System with EOL, please log in to my.utrgv.edu and submit a ticket through Service Now or contact the IT Service Desk as soon as possible.

Brownsville / Harlingen / South Padre Island 956-882-2020

Edinburg / McAllen / Rio Grande City 956-665-2020

A friendly recommendation for students, faculty, and staff that use personal computers or laptops: Please review the following systems requirements, log in to my.utrgv.edu, visit the vSoftware application, and purchase ($9.95 USD) Windows 10; it is highly recommendable that you back up all of your files, photos, and any other important documents before you upgrade your OS. In the case that your personal computer does not support the OS, please consider upgrading your machine.

For more EOL software please visit: bit.ly/list-EOL2017

# CLEAN DESK SECURITY BEST PRACTICE


*An example of a BAD practice*

A clean desk practice ensures that all sensitive/confidential materials are removed from an end user workspace and locked away when the items are not in use or an employee leaves his/her workstation. It is one of the top strategies to utilize when trying to reduce the risk of security breaches in the work-place. Please use the checklist below daily to ensure your work (or home) workspace is safe, secure, and compliant.

- ☐ Passwords should not be left written down in any accessible location.
- ☐ Ensure all sensitive/confidential information in hardcopy or electronic form is secure at the end of the workday or when you will be gone for an extended period.
- ☐ Computer (laptops, tablets, phones, etc.) screens should be locked when the workspace is unoc-cupied.
- ☐ Portable computing devices such as laptops, tablets and mobile phones should be secured in locked storage when not attended or at the end of the workday.
- ☐ External storage devices such as CD's, DVD's, or USB drives should be secured in locked storage when not in use or not attended.
- ☐ File cabinets, drawers and storage lockers containing Confidential or Sensitive information should be kept closed and locked when not in use or not attended.
- ☐ Keys used for access to Confidential or Sensitive information should not be left at an unattended desk
- ☐ All printers and fax machines should be cleared of papers as soon as they are printed; this helps ensure that Confidential or Sensitive documents are not left behind for the wrong person to pick up.
- ☐ Upon disposal*, Confidential and/or Sensitive documents should be shredded or placed in locked confidential disposal bins.

**Ensure UTRGV record management and retention policies are followed when disposing of any UTRGV official records [HOP ADM-10-102]*

# ISO Spotlight

The ISO Spotlight interviews an individual that plays a role in UTRGV and information security. In this issue, you will meet *Department Chair Ph.D. Jerald Hughes* of Information Systems in the Robert C. Vackar College of Business & Entrepreneurship.

## *Ph.D. Jerald Hughes*

***Department Chair***

**1. Tell us how information security has changed since you started in your role.**
It has both broadened and deepened--many more ways/chances to be attacked; some much easier ways, some much harder, many more motivations, many more needs to defend.

**2. Who are your customers, and what is one of the most challenging areas for you?**
In the university, students - most challenging is trying to find ways to bring together such broad information domains--so much to know, in order to *understand why things happen.*
In business community, local banks and local non-profits: Banks are highly attuned to risk already, biggest challenge there is to find right balance of Simplicity and Security. Very lengthy security protocols significantly slow down the work.
Non-profits are barely able to assemble any resources for security; biggest challenge is to just get started on minimum appropriate procedures and IT.

**3. How did you come into the security field?**
Interest in multimedia - Napster was a huge break with history, showing what was possible with information goods. Cracks against data formats, application protections, Digital Rights Management generally. To understand how those worked and the strategic forces involved, had to go fully into information security.

**4. Top 3 life highlights:**

- Family, of course-- wife and 2 daughters, who make me happy every day.
- Education, of course, I hold a Doctor of Musical Arts in music composition, and a PhD in Business Information Systems.
- Aside from those, travel experiences: drove to Aspen Colorado for music festival four times, two trips to Germany, Singapore, Bangkok, lived in New York City--seeing the world.

**5. People would be surprised to know:**
I am a musician –operatic tenor, piano, guitar. I compose electronic music.

**6. Which CD do you have in your car? Or what radio station do you listen to?**
Yasutaka Nakata's techno group capsule: albums Caps Lock and Wave Runner; otherwise lots of classical CD's: Bach, Ravel, Beethoven.

**7. If you could interview one person (dead or alive) who would it be?**
Philosopher Daniel Dennett, author of "Consciousness Explained"

**8. If given a chance, who would you like to be for a day?**
Ben Heppner, operatic tenor, who sang "Tristan und Isolde" with the Metropolitan Opera

**9. What is the best advice that you have received and that you have used?**
Advice from the chair of my Information Systems doctoral dissertation committee: "Make yourself the world expert on this particular topic. Your job now is to make your *own decisions* about how to understand it, how to research it, how to solve problems in this area." This was my biggest transition from the student point of view to the professional point of view.

**10. What would be your advice for a new security professional?**
Think like a Black Hat! The bad guys in Information Security was spectacularly good at thinking outside the box, at doing the unexpected. The security field moves so quickly, and new threats pop up in so many places, that a security pro's best approach is to understand, and practice, how the bad guys are approaching each new opportunity in hardware, software, systems.

***Featured Article***

*By Francisco Tamez*
*UTRGV Security Analyst*

## Time for some digital storage

Many, if not all, users regularly save a backup of their files to the computer; by doing this you are not as susceptible to lose all your data. Unfortunately computer crashes always take place when you need the information most:

- Hard drives have a finite lifetime and can fail suddenly and without warning,
- Physical laptop damage can cause the painful loss of months (or years) of irreplaceable files and photos,
- Virus infection of aggressive malicious viruses can corrupt files and disable computers.

The solution to all of these is having duplicate copies of your most important information. Fortunately, all UTRGV students, staff, and faculty can rely on 1 TB of OneDrive for Business storage.

OneDrive for Business is a free cloud storage service provided by UTRGV to students and employees which will let you get to your files from anywhere with a network connection on any compatible device. Furthermore, it will allow you to share and work together with anyone in your educational, professional, or personal life. Simply log in to www.my.utrgv.edu, select the Office 365 application and click on OneDrive. Once you have open your OneDrive, you can Sync any library from your device for easy access. By syncing your files you will be able to review the updated version of your document from any device affiliated to your OneDrive account.

With 1TB of cloud storage, you can work together and collaborate with Word, Excel, PowerPoint, and OneNote from your desktop, mobile device, and the web. The collaborative advantage of using this service is that you can give others permission to edit files and work on them at the same time. You can also see the comments made when files are uploaded into the libraries.

You can also view or restore previous versions of documents in OneDrive for Business (as long as you haven't turned off document versioning). Versioning is very resourceful when you just want to view an earlier document version without overwriting your current version. Alternatively, you may want to see and compare an earlier document version before you restore it as the current version in the case that you made a mistake, if the current version is corrupt, or if you simply like a previous version better. Similarly, when versioning is enabled in your list or library, you can see when a file was changed and who changed it. All of these features together make OneDrive an excellent backup source for data files.

Whether you save your files to CDs or DVDs, a cloud back-up service (e.g., One Drive), or an external hard drive, spring cleaning is a great time to verify you have a complete backup of all your important files and pictures.

Feel free to visit Microsoft's website for a quick overview of OneDrive (bit.ly/MOneDrive).

For more information on how to create a backup Sync library folder in OneDrive please visit UTRGV IT website: www.utrgv.edu/it/how-to/

*Security NOTE:* OneDrive for Business provided by UTRGV is the only cloud storage service that is approved to store university owned data, any other personal obtained cloud storage service (e.g., Google Drive, DropBox) is prohibited. For more information please review the Information Resources Acceptable Use and Security Policy (AUP)

# ISO GUEST


## SPRING TIME! Review Your Safety Checklist!

### Smoke Alarms

According to NFPA three out of every five home fire deaths result from homes with no smoke alarms.
Smoke alarm maintenance is crucial in order to obtain full benefit. Fire alarms should be tested every month to make sure they are working properly. In addition, batteries should be replaced at least once a year.

If installing new smoke alarms:

- Mount them at least 10 ft. from the stove to prevent false alarms
- Mount them less than 12 inches from the ceiling and away from windows, doors and ducts

It is recommended that all smoke alarms are interconnected wirelessly so that when one alarm goes off they all do and everyone can be aware.

### Carbon Monoxide Detectors

When installing carbon monoxide alarms be sure to install them in a central location outside bedrooms and on every level of the home.

It is important to replace batteries at least once a year and to test them at least once every month, just as smoke alarms.

Cleaning out vents for gas appliances is also important, such appliances are:

- Dryer
- Stove
- Furnace
- Fireplace

Keep an eye out for snow or debris!

## Family Emergency Plan

It is recommended for your family to have an emergency plan and a home/car emergency kit in place in the event of a natural disaster or other catastrophic event.

Some things to include in an emergency kit are:

- 1 gallon of water per person for each day
- 3-day supply food
- Flashlight
- First-aid kit
- Filter mask
- Medicines

## What Else Should You Do?

As you're spring cleaning take unwanted or expired medicines to a prescription drop box, discard any chemicals/household cleaners that are labeled with an expiration date and update your first aid kit.

## Emergency Contacts

**University Police**
Brownsville:
(956)882-8232 (main)
(956)882-2222 (emergency)

Edinburg:
(956)665-7151
Harlingen:
(956)882-7232

**Env. Health, Safety & Risk Management**
(956)882-5930 (Brownsville)
(956)665-3690 (Edinburg)

**Facilities Operations**
(956)665-2770

**Emergency 911**

## The Office of Emergency Preparedness

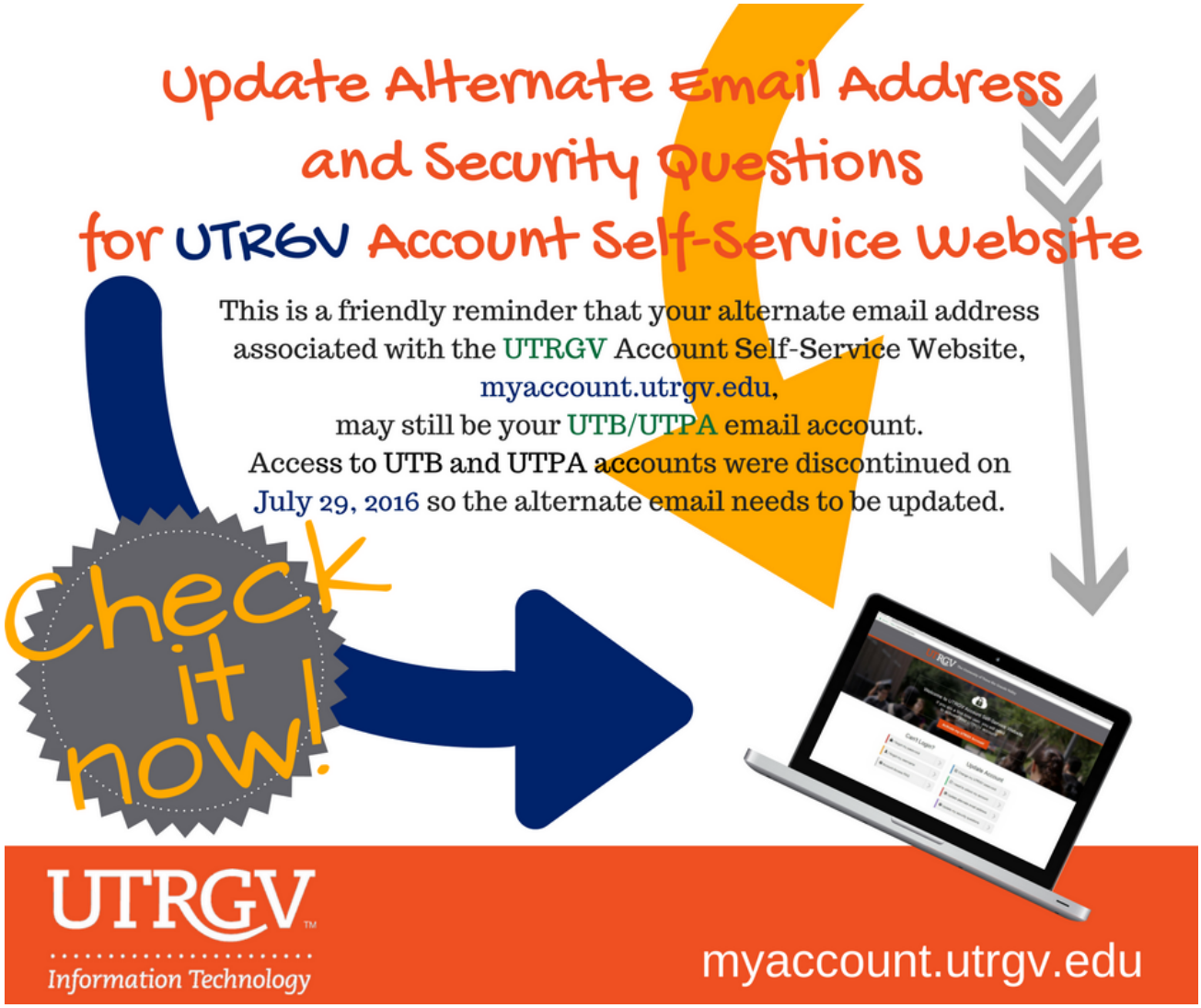
- Promotes a foundation for emergency management and provides the framework for effective preparedness efforts through the Emergency Operations Plan and related annexes;
- Maintains, develops and aligns achievable emergency management goals and objectives with the vision, mission, and purpose of The University of Texas Rio Grande Valley;
- Defines procedures pertinent to the execution of the Emergency Management Program;
- Identifies, and maintains good working relationships with internal and external emergency management partners and stakeholders; and
- Strengths program continuity and viability by providing training and exercises.

**Office of Emergency Preparedness Contact Information**
(956)665-2658
emergencypreparedness@utrgv.edu
www.utrgv.edu/emergencypreparedness

Do **YOU** have an idea for a topic? Would you like to include something in particular to this newsletter? Any comments or suggestions are **ALWAYS** welcome!

Feel free to submit your thoughts by visiting our website:

bit.ly/utrgvisonewsletterfeedback




DON'T
GET
SMACked
Check your
Social Media
Access Controls
utrgv.edu/is/en-us/
resources/social-media


WE
ARE
SOCIAL!
www.utrgv.edu/is
www.facebook.com/utrgviso

# NEWSWORTHY SECURITY ARTICLES

**FDA slams St. Jude on device security**
The U.S. Food and Drug Administration issued a letter of warning to medical device maker Abbott on Wednesday, slamming the company for what it said was a pattern of overlooking security and reliability problems in its implantable medical devices at its St. Jude Medical division and describing a range of the company's devices as "adulterated," in violation of the US Federal Food, Drug and Cosmetic Act. (bit.lyfdaslamsstjude)

**Texas 10th grader hacks school network to change grades**
A Texas high school sophomore was arrested on March 31 and charged with a felony for hacking into the Spring Branch Independent School District computer system in order to change student's grades. (bit.ly/texastengraderhacksschool)

These and other articles can be found at: bit.ly/UTRGVISOnewsnalerts


## If you need to report an incident

Visit our website (www.utrgv.edu/is) if you need to report a security incident. Some incidents may require you to report them to both the ISO and the UTRGV Police Department (PD) or to Information Technology (IT). For example any loss or theft of a University owned computer (e.g. workstation, laptop, smartphone, tablet) has to be reported to the ISO and the UTRGV PD. Similarly, ransomware infected UTRGV owned computers must be reported to ISO and IT.

REPORT INCIDENT

The University of Texas Rio Grande Valley™

Information Security Office

The mission of the Information Security Office is to provide support to the University in achieving its goals by ensuring the security, integrity, confidentiality, and availability of information resources. The role of the Chief Information Security Officer (CISO) is to maintain oversight and control of the enterprise information security program for the University.

**Locations:**

- Sugar Road Annex (ESRAX) Building
- R-167 Rusteberg Hall (BRUST) Building (*by appointment*)

**Phone:** (956)665-7823

**Email:** is@utrgv.edu

Visit us on the web and social media!
www.utrgv.edu/is www.facebook.com/utrgviso

### Services We Provide

GOVERNANCE, RISK AND COMPLIANCE

ASSET AND VULNERABILITY MANAGEMENT

ENGINEERING AND INCIDENT RESPONSE

AWARENESS, COMMUNICATION AND OUTREACH

**Give us YOUR FEEDBACK!**
bit.ly/utrgvisonewsletterfeedback

## Special Thanks To:

| Safety and Security | Information Technology | Office of the President |
|---|---|---|
| Julia Gonzalez | Irma Hermida and Hilda Gonzalez | Anai Perez |