The Texas A&M University System is replacing various legacy mainframe payroll and human resource systems with one unified system called ***Workday.***

The A&M System will benefit from *Workday*'s intuitive, web-based applications with self-service and mobile capabilities. *Workday* is designed to work the way we work today and will help create a more nimble, process and data driven organization.

Workday will replace many of the current Single Sign-On applications. It will launch in December 2017 with the following modules: HCM (Core HR), Compensation, Benefits, Payroll, Recruiting, Absence, Time Tracking, Reporting, Talent Management, and Performance Management.

Workday News & Updates

- Videos
  - Say Hello to Workday
  - Say Hello to Workday: Employees
  - Say Hello to Workday: HR, Payroll and Benefits Employees
  - Say Hello to Workday: Managers
- "*The Word on Workday*"
- What's Going, What's Staying
- Security Roles
- Questions and Answers
- TAMUS to Workday Terminology & Definitions

Workday Training Opportunities

- TrainTraq courses on General Awareness, Targeted Awareness and Hands-on Skills will be available beginning in September and October
- The Texas A&M University System Workday Training Course Catalog and Video Help Release Schedule provides information on training courses currently in development
- Drop-in Learning Labs are scheduled for November 9th through 14th

---

Change Impacts

- Save for Summer will replace the Extended Pay Plan beginning January 2018
- Biweekly Pay Periods will change to run from Sunday to Saturday beginning September 1st

---

Data Protection in the Cloud: The Workday Way

Protecting and securing customers' data is fundamentally important to Workday. Privacy and security at Workday are not add-on features; they are embedded in our service and business model. All Workday customers are always on the same version of our software. This enhances our ability to innovate and our ability to protect our customers' data. We can respond to security threats quickly by pushing security updates to our entire customer base and ensuring common data handling standards. We also operate on a unified security model. This includes user access, system integration, reporting, mobile device, and IT access.

Workday is committed to key security and privacy concepts that promote a secure, safe regulated environment:

- **Our customers own and control their data.** We only use customer data to operate our service and don't monetize the data. Each customer determines what data to enter and configures the applications to best safeguard their data and can configure business processes to further safeguard the privacy of personal data.
- **Data is encrypted when it is in transit and at rest in our persistent data store.** Workday encrypts every attribute value in the application before it is stored in the database. This is a fundamental design characteristic of the Workday technology. All customer data in the persistent layer is encrypted and accessed only by the application server.
- **We are transparent about where and how customer data is processed.** We provide customers with visibility to our security and privacy controls through third-party audits (SOC-1 and SOC-2), through ISO (27001 and 27018), Safe Harbor and TRUSTe Enterprise certifications, as well as our Customer Audit Program.

If you have questions about *Workday* please contact:

***Workday* Change Champion**
Jeff Boyer | boyerj@tamug.edu | 409-740-4503

***Workday* Project Coordinator**
Tina Pennington | penningt@tamug.edu | 409-740-4534