𝐃 Finance & Admin Update

The latest news, updates, and announcements from Finance, Finance Centers, Campus Services, Human Resources, Information, Technology & Consulting, Integrity & Compliance, Internal Controls Services, and Safety & Security

Chart of the Month

Hires Submitted 5 Days Prior to and After Effective Date
(January – June 2024)
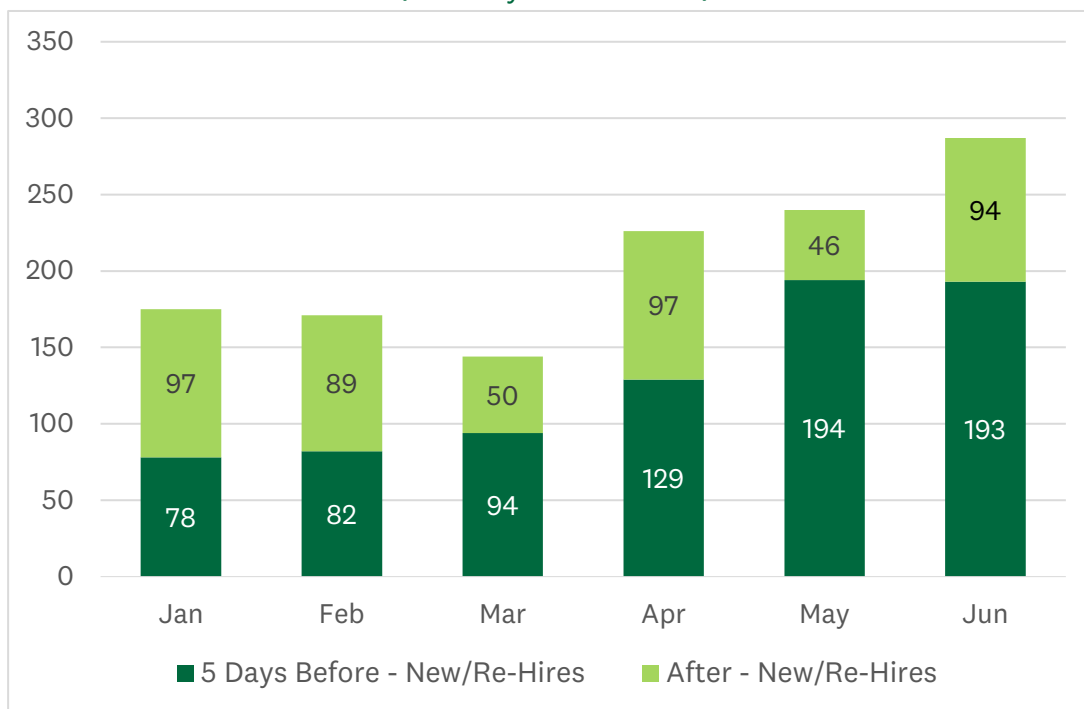
Source: PASF New Hires and Rehires (January 1 – June 30, 2024)

Over the past six months, Dartmouth has welcomed 1,243 new employees, with 770 Personnel Authorizations submitted at least five days in advance of the employees' start date. Early submission helps to ensure that the employees' information is processed within our systems for payroll, benefits, email, notifications, and other job critical accesses such as system access, ID Cards, and parking. Hiring employees on time sets the stage for a more successful onboarding and overall employee experience from day one.

However, nearly 40 percent of newly hired and re-hired employees did not have their basic employee profiles and access set up in advance, resulting in a less smooth onboarding experience. To address this, Finance, in collaboration with HR, has updated the Recruitment and Hiring site. This site now includes additional resources to guide hiring managers and departments through a more inclusive and successful recruitment and hiring process, as detailed in the "Before You Begin" section. Additionally, we have updated the Onboarding Checklist to help hiring managers and peer partners plan and prepare for an exceptional onboarding experience. *(continued in Onboarding and Offboarding on page 2)*

Upcoming Dates

Agiloft Contract
Management Training
Thursday, July 25,
1:30 – 3:15PM
———
Finance Collaborative
Wednesday, August 7,
9:00 – 10:00AM

Finance Staff Update

Congratulations to **Amelia Parizo**, who recently joined the Endowment & Investment Accounting team, as the Endowment and Investment Accounting Analyst.

Onboarding and Offboarding
(continued from page 1)

Just as timely onboarding is crucial, so is the timely termination of employment. Of the 877 terminations and retirements submitted between January and June 2024, 62 percent of those were submitted 5 days prior to the termination date. Failing to terminate and properly offboard employees on time can result in continued access facilities, resources, and systems, delayed processing of benefits, and an increased risk of payroll overpayment.

To assist managers and employees in ending employment with Dartmouth, we have updated the Offboarding Checklists. The Offboarding Checklist for Managers outlines the essential activities necessary for proper termination and offboarding, such as submitting the termination request and canceling procurement or corporate cards. Additionally, the Employee Ending Employment Checklist guides employees through returning Dartmouth equipment, ID, and credit cards, setting up an email autoreply, reviewing and updating their employee self-services, and reviewing benefits.

Agiloft IRA Reports

Agiloft IRA Reports are now available for those with access to IRA Financial Reports. These reports provide visibility into accounts payable spending and the remaining balance of your Agiloft agreements. You can find these reports in the Procurement section of your IRA Launchpad.

Note that the accuracy of these reports depends on the information entered into the Agiloft Contract Management System and the Payment Request eForm. For example, if payment information is missing in the IRA report, it might be due to missing or incorrect information provided on the Payment Request eForm.

Please review these reports and provide us with your feedback. If you find any incorrect or missing information when reviewing your reports, please send a note with any information, if available, to Agiloft.Help@Dartmouth.edu and we will research and update it in the various systems and reports.

Terminations Submitted 5 Days Prior to/After Effective Date
(January – June 2024)
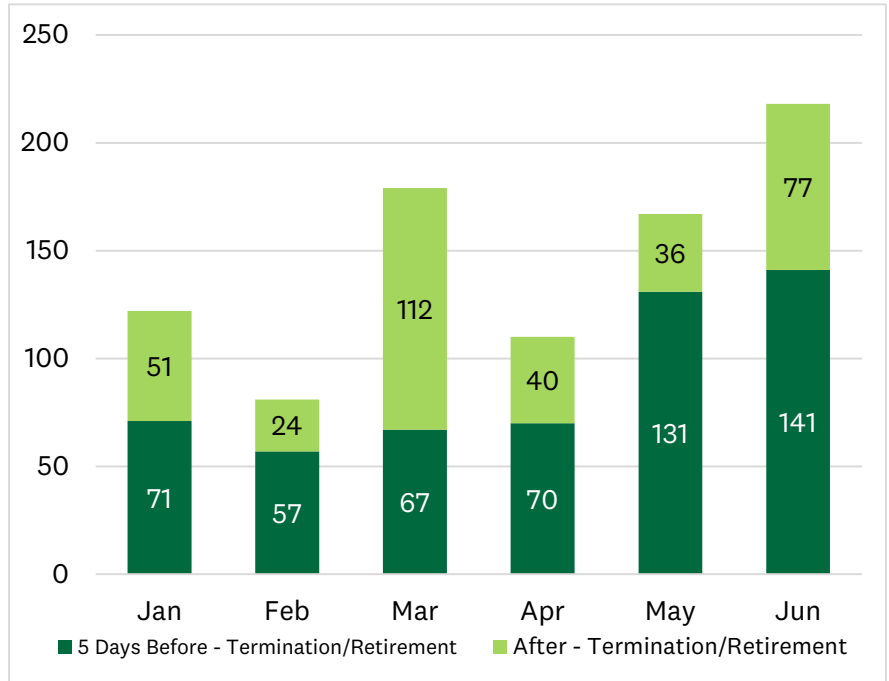
Source: PASF Termination/Retirement (January 1 – June 30, 2024)

Policy Updates Now Available

The Business Expense Policy and Signature Authority Policy, effective July 1, 2024, are now available within the Policy Portal.

OnBase Upgrade Coming

The OnBase Unity Client is being upgraded. The testing of the new client has begun, and we anticipate the upgrade to begin Thursday, August 15th through Friday, August 16th. During the upgrade, the OnBase Unity Client and eForms will be unavailable. Anyone using the desktop client should have the pushed directly to your computer. If this does not occur by Monday, August 19th, you will be able to find the new version within the Dartmouth Software Center. For those using RDS, the client will be updated automatically.

Upcoming System Training

⛭ Agiloft Contract Management Training
- Thursday, July 25, 1:30 – 3:15PM
- Thursday, August 22, 1:30 - 3:15PM

🔵 OnBase Unity Client: Getting Started
- Wednesday, July 24, 9:00 – 10:00AM
- Wednesday, September 11, 9:00 – 10:00AM

Cybersecurity Starts with Physical Security

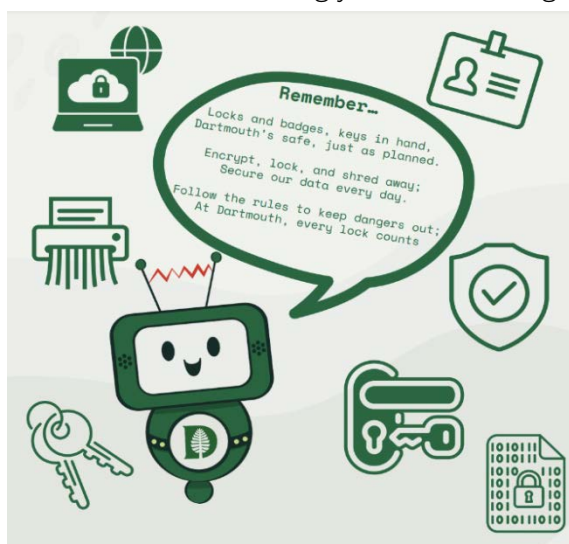*By Leslie Athena Kelton, Matthew Gilliland and Sean McNamara, Information Technology and Consulting*

Dartmouth's first line of defense in cybersecurity starts with keeping those hallowed doors locked! Dartmouth's Access Control Policy highlights how you can help keep our campus and technology secure. The following are the policy highlights and how you can help keep our campus safe. Every lock counts at Dartmouth!

Dartmouth's physical access control policy

- Establishes a standard for academic or administrative purposes for Dartmouth Facilities, requiring electronic access controls for all exterior doors.
- Authorized users are granted access via an electronic access control system, which uses a combination of physical controls and identification processes to manage access to Dartmouth facilities.

ID Badges

- Protect all ID badges, access cards, and keys.
- Do not share access credentials.
- Report any misplaced access items immediately.
- Always use your own ID badge when entering a secure area.
- Avoid tailgating - entering a secured entryway behind someone else without using your own ID badge.

Devices

- All devices should be passcode/password protected.
- Lock the screen on your device when away from your desk.
- Device encryption
- Encryption should be enabled on all devices used for work.
- All devices managed through Dartmouth's Device Assurance Program (DAP) have encryption enabled by default.
- If you are uncertain whether your device is enrolled in DAP or need assistance turning on disk encryption on a device, you can submit a request for assistance.
- Keep track of your devices when traveling or in public places.
- If your device is stolen or goes missing, report it immediately via TDNext or by sending an email to information.security@dartmouth.edu

Documents and Sensitive Information

- When you leave for the day, make sure any sensitive documents or drives are locked up.
- Remove sensitive information from whiteboards and tables in private and shared spaces.
- Immediately pick up any documents after they are printed or copied.
- Shred sensitive documents when you no longer need them.
- Limit physical access to sensitive documents so only those who need access have it.
- Maintain a record of all devices, physical documents, etc., that contain sensitive information.

By following the guidelines above, you play a crucial role in protecting sensitive information from unauthorized access. We can all take proactive steps to strengthen our physical security measures.