FAIRLEIGH DICKINSON UNIVERSITY

Information Resources and Technology

FDU PROCEDURE ON HANDLING DATA ON SEPARATING EMPLOYEES

Responsible Office:	OIRT / Human Resources	Effective Date: 03/15/2021
Responsible Official:	Neal Sturm, VP & CIO	
	Rose D'Ambrosio, VP, HR	Last Revision: 03/15/2021

I. OBJECTIVE

Create a standard procedure by which Manager's and their employee's transfer University data during the period of time from when an employee makes their intention clear that they are separating from the University or the transfer of University data at the time of an employee's involuntary separation from the University.

II. PROCEDURES

Voluntary Separation

It is the manager or direct supervisor's responsibility to work with the separating employee to extract any data or files that reside locally on their computer that would be needed for business continuity. The supervisor should also ensure they understand what shared drives the separated employee used and have access to those drives if need be.

Using appropriate security precautions, the manager should meet several times with the separating employee to ensure all information is transferred over either email, a shared drive, One Drive or a thumb drive.

During the separation process, through the Employee Separation Checklist, the employee's manager can select the ability to access the separating employee's email for up to 30 days and/or forward emails addressed to the separated employee for up to 60 days.

Upon receiving the separation notice, Computing Services will validate through our Backup system that the separating employee's complete laptop or desktop Image has been backed up.

Computing Services will manually trigger an additional backup within three days of separation.

Immediately upon the effective date of the separation, the separating employee's manager is responsible for turning over the separating employees' computer to Computing Services.

Computing Services will store the computer for 14 days as a precaution, and then wipe the data from that computer, reimage the computer, and shelf the computer for redistribution.

If it is discovered that information that resided on the separated employee's computer was missed during the separation process and needs to be retrieved at a later point, the supervisor would need to contact the Vice President of Human Resources and request the specific data that would need to be recovered from our Backup system.

Involuntary Separation

Upon the dismissal of the individual, Human Resources, would immediately engage Computing Services as well as the direct supervisor to view and extract any data that might be needed by the department to ensure business continuity. This would take place as soon as possible from the date of dismissal.

If a legal hold is required, Computing Services and USAN would be notified and the existing processes of extracting and encrypting the hard drive as well as protecting all email correspondence would be executed. Computing Services would then remove the computer.

If a legal hold is not required, Computing Services will validate through our Backup system that the dismissed employee's Image has been properly backed up and remove the computer.

Computing Services will store the computer for 14 days as a precaution, and then wipe the data from that computer, reimage the computer, and shelf the computer for redistribution.

If it is discovered that information that resided on the separated employee's computer was missed during the separation process and needs to be retrieved at a later point, the supervisor would need to contact the Vice President of Human Resources and request the specific data that would need to be recovered from our Backup system.

III. IN CASE OF QUESTIONS

Questions regarding this procedure can be directed to the Vice President of Human Resources.