Standards for Granting and Removing Access to Information Resources:
Guide for Departments

Standards for Granting and Removing IT Access								
Guide for Departments								
revised 10/21/13								
Service	**User Type**	**Employment Status**	**Position Information**	**Action to be Taken**	**Minimum Access to be Enabled**	**Duration**	**Initiator/Requester**	**Service Provider(s) and Approver(s)**
EIS								
	Employee	New Hire	not applicable	conduct administrative review of access privileges based on function of position	conduct administrative and security review of access needs based on function of position; enable access based on outcome of review	as applicable to the function of the position	supervisor and/or department head	EIS ACES, information owner(s)
	Employee	Termination	permanent	disable access	none; disable all roles except EIS self-service	permanent	supervisor and/or department head	EIS ACES, information owner(s)
	Employee	Classification Change (promotion, transfer, demotion, etc.)	internal department	conduct administrative review of access privileges based on function of new classification; remove access privileges that are not needed for new classification	conduct administrative and security review of access privileges based on function of new classification; enable access based on outcome of review	based upon administrative and security review; remove access privileges that are not needed for new classification	previous and new supervisors and/or department heads	Previous and new EIS ACES, information owners
	Employee	Classification Change (promotion, transfer, demotion, etc.)	external department	disable all roles	none; disable all roles except EIS self-service	permanent	previous and new supervisors and/or department heads	Previous and new EIS ACES, information owners
	Employee	Retirement	permanent	disable all roles	none; disable all roles except EIS self-service	permanent	supervisor and/or department head	EIS ACES, information owner(s)
	Employee	Leave-of-Absence, Administrative Leave	internal department	conduct administrative review of access privileges based on nature of absence	conduct administrative and security review of access needs based on function of position; enable access based on outcome of review	based upon administrative review; if appropriate, retain for duration of leave; maximum retention period is 3 months; remove access for periods that exceed 3 months	supervisor and/or department head	EIS ACES, information owner(s)
	Employee	Modified Service, Other Types of Service	internal department	conduct administrative review of access privileges based on function; remove access privileges that are not needed for function	conduct administrative and security review of access needs based on function of position; enable access based on outcome of review	based upon administrative and security review; remove access privileges that are not needed for new classification	supervisor and/or department head	EIS ACES, information owner(s)
	Person-of-Interest	non-employee, contractor, consultant, guest, visiting scholar, vendor	legal contract or written agreement required between institution and person-of-Interest required	conduct administrative review of access privileges based contract or written agreement; remove access privileges when agreement expires or terminates	conduct administrative and security review of access privileges based contract or written agreement; enable access based on requirements of contract or written agreement	per contract or written agreement between institution and person-of-interest; remove all access privileges when agreement expires or terminates.	supervisor and/or department head	ITSS Security functions, IT manager, EIS ACES, information owner(s)
Network Account(s), Departmental Computer Systems and Other Applications								
	Employee	New Hire	not applicable	conduct administrative review of access privileges based on function of position	conduct administrative and security review of access needs based on function of position; enable access based on outcome of review	as applicable to the function of the position	supervisor and/or department head	IT manager(s), resource manager(s), resource owner(s)
	Employee	Termination	permanent	disable all access	none	permanent	supervisor and/or department head	IT manager(s), resource manager(s), resource owner(s)
	Employee	Classification Change (promotion, transfer, demotion, etc.)	internal department	conduct administrative review of access privileges based on function of new classification; remove access privileges that are not needed for new classification	conduct administrative and security review of access privileges based on function of new classification; enable access based on outcome of review	based upon administrative and security review; remove access privileges that are not needed for new classification	previous and new supervisors and/or department heads	Previous and new IT managers, resource manager(s), and resource owner(s)

Standards for Granting and Removing Access to Information Resources:
Guide for Departments

Service	User Type	Employment Status	Position Information	Action to be Taken	Minimum Access to be Enabled	Duration	Initiator/Requester	Service Provider(s) and Approver(s)
	Employee	Classification Change (promotion, transfer, demotion, etc.)	external department	disable all access	none	permanent	previous and new supervisors and/or department heads	Previous and new IT managers, resource manager(s), and resource owner(s)
	Employee	Retirement	permanent	disable all access	none	permanent	supervisor and/or department head	IT manager(s), resource manager(s), resource owner(s)
	Employee	Leave-of-Absence, Administrative Leave	internal department	conduct administrative review of access privileges based on nature of absence	conduct administrative and security review of access needs based on function of position; enable access based on outcome of review	based upon administrative and security review; if appropriate, retain for duration of leave; maximum retention period is 3 months; remove access for periods that exceed 3 months	supervisor and/or department head	IT manager(s), resource manager(s), resource owner(s)
	Employee	Modified Service, Other Types of Service	internal department	conduct administrative review of access privileges based on function; remove access privileges that are not needed for function	conduct administrative and security review of access needs based on function of position; enable access based on outcome of review	based upon administrative and security review; if appropriate, retain for duration of leave; maximum retention period is 3 months; remove access for periods that exceed 3 months	supervisor and/or department head	IT manager(s), resource manager(s), resource owner(s)
	Person-of-Interest	non-employee, contractor, consultant, guest, visiting scholar, vendor	legal contract or written agreement required between institution and person-of-Interest required	conduct administrative review of access privileges based contract or written agreement; remove access privileges when agreement expires or terminates	conduct administrative and security review of access privileges based contract or written agreement; enable access based on requirements of contract or written agreement	per contract or written agreement between institution and person-of-interest; remove all access privileges when agreement expires or terminates.	supervisor and/or department head	IT manager, ITSS Information Security,information owner(s), resource manager
	Supervisor or Department Head	Employee Absence or Termination	request for access to employee files; requester is supervisor of employee	conduct administrative review of access privileges based on employee function; remove access privileges that are not needed for employee function	conduct administrative and security review of access needs based on function of position; enable access based on outcome of review	30 or 60 day access based on administrative and security review	supervisor and/or department head	ITSS Information Security; information owner(s), system owner(s), resource owner(s), resource manager
Email								
	Employee	New Hire	not applicable	conduct administrative review of access privileges based on function of position	conduct administrative and security review of access needs based on function of position; enable access based on outcome of review	as applicable to the function of the position	supervisor and/or department head	IT manager
	Employee	Termination	permanent	disable all access	none	permanent	supervisor and/or department head	IT manager
	Employee	Classification Change (promotion, transfer, demotion, etc.)	internal department	conduct administrative review of access privileges based on function of new classification; remove access privileges that are not needed for new classification	conduct administrative and security review of access privileges based on function of new classification; enable access based on outcome of review	based upon administrative and security review; remove access privileges that are not needed for new classification	previous and new supervisors and/or department heads	Previous and new IT managers
	Employee	Classification Change (promotion, transfer, demotion, etc.)	external department	disable access; email account may be transferred, but data remains property of previous department	none	permanent	previous and new supervisors and/or department heads	Previous and new IT managers
	Employee	Retirement	permanent	disable access; retirees may be eligible to retain email access per provisions of the institutional computer use or acceptable use policies; email account may be transferred, but data remains property of previous department	none	based upon administrative and security review	supervisor and/or department head	IT manager

Standards for Granting and Removing Access to Information Resources:
Guide for Departments

Service	User Type	Employment Status	Position Information	Action to be Taken	Minimum Access to be Enabled	Duration	Initiator/Requester	Service Provider(s) and Approver(s)
	Employee	Leave-of-Absence, Administrative Leave	internal department	conduct administrative review of access privileges based on nature of absence	conduct administrative and security review of access needs based on function of position; enable access based on outcome of review	based upon administrative and security review; if appropriate, retain for duration of leave; maximum retention period is 3 months; remove access for periods that exceed 3 months	supervisor and/or department head	IT manager
	Employee	Modified Service, Other Types of Service	internal department	conduct administrative review of access privileges based on function; remove access privileges that are not needed for function	conduct administrative and security review of access needs based on function of position; enable access based on outcome of review	based upon administrative and security review; if appropriate, retain for duration of leave; maximum retention period is 3 months; remove access for periods that exceed 3 months	supervisor and/or department head	IT manager
	Person-of-Interest	non-employee, contractor, consultant, guest, visiting scholar, vendor	legal contract or written agreement required between institution and person-of-Interest required	conduct administrative review of access privileges based contract or written agreement; remove access privileges when agreement expires or terminates	conduct administrative and security review of access privileges based contract or written agreement; enable access based on requirements of contract or written agreement	per contract or written agreement between institution and person-of-interest; remove all access privileges when agreement expires or terminates.	supervisor and/or department head	IT manager, ITSS Information Security, information owner(s), resource manager
	Supervisor or Department Head	Employee Absence or Termination	request for access to employee files; requester is supervisor of employee	conduct administrative review of access privileges based on employee function; remove access privileges that are not needed for employee function	conduct administrative and security review of access needs based on function of position; enable access based on outcome of review	30 or 60 day access based on administrative and security review	supervisor and/or department head	ITSS Information Security, information owner(s), system owner(s), resource owner(s), resource manager
Physical Access to Information Resources (office computers, keys, combination/keypad locks, biometric clocks, burglar alarm IDs, UNT ID cards/badges, etc.)								
	Employee	New Hire	not applicable	conduct administrative review of access needs based on function of position	conduct administrative and security review of access needs based on function of position; enable access based on outcome of review	as applicable to the function of the position	supervisor and/or department head	Departmental designee(s) for physical security, Door Systems (UNT and UNT System only), Police Department (UNT Dallas only), resource manager
	Employee	Termination	permanent	disable all access	none	permanent	supervisor and/or department head	Departmental designee(s) for physical security, Door Systems (UNT and UNT System only), Police Department (UNT Dallas only)
	Employee	Classification Change (promotion, transfer, demotion, etc.)	internal department	conduct administrative review of access privileges based on function of new classification; remove access privileges that are not needed for new classification	conduct administrative and security review of access privileges based on function of new classification; enable access based on outcome of review	based upon administrative and security review; remove access privileges that are not needed for new classification	previous and new supervisors and/or department heads	Previous and new departmental designee(s) for physical security, Door Systems (UNT and UNT System only), Police Department (UNT Dallas only)
	Employee	Classification Change (promotion, transfer, demotion, etc.)	external department	disable all access	none	permanent	previous and new supervisors and/or department heads	Previous and new departmental designee(s) for physical security, Door Systems (UNT and UNT System only), Police Department (UNT Dallas only)
	Employee	Retirement	permanent	disable all access	none	permanent	supervisor and/or department head	Departmental designee(s) for physical security, Door Systems (UNT and UNT System only), Police Department (UNT Dallas only)
	Employee	Leave-of-Absence, Administrative Leave	internal department	conduct administrative review of access privileges based on nature of absence	conduct administrative and security review of access needs based on function of position; enable access based on outcome of review	based upon administrative and security review; if appropriate, retain for duration of leave; maximum retention period is 3 months; remove access for periods that exceed 3 months	supervisor and/or department head	Departmental designee(s) for physical security, Door Systems (UNT and UNT System only), Police Department (UNT Dallas only)

Standards for Granting and Removing Access to Information Resources:
Guide for Departments

Service	User Type	Employment Status	Position Information	Action to be Taken	Minimum Access to be Enabled	Duration	Initiator/Requester	Service Provider(s) and Approver(s)
	Employee	Modified Service, Other Types of Service	internal department	conduct administrative review of access privileges based on function; remove access privileges that are not needed for function	conduct administrative and security review of access needs based on function of position; enable access based on outcome of review	based upon administrative and security review; if appropriate, retain for duration of leave; maximum retention period is 3 months; remove access for periods that exceed 3 months	supervisor and/or department head	Departmental designee(s) for physical security, Door Systems (UNT and UNT System only), Police Department (UNT Dallas only)
	Person-of-Interest	non-employee, contractor, consultant, guest, visiting scholar, vendor	legal contract or written agreement required between institution and person-of-Interest required	conduct administrative review of access privileges based on function; remove access privileges that are not needed for function	conduct administrative and security review of access privileges based contract or written agreement; enable access based on requirements of contract or written agreement	per contract or written agreement between institution and person-of-interest; remove all access privileges when agreement expires or terminates.	supervisor and/or department head	IT manager; ITSS Information Security; information owner(s); resource manager
Other Systems (Research systems, etc.)								
	Employee	New Hire	not applicable	conduct administrative review of access privileges based on function of position	conduct administrative and security review of access needs based on function of position; enable access based on outcome of review	as applicable to the function of the position	supervisor and/or department head; or system owner	IT manager or resource owner
	Employee	Termination	permanent	disable all access	none	permanent	supervisor and/or department head; or system owner	IT manager or resource owner
	Employee	Classification Change (promotion, transfer, demotion, etc.)	internal department	conduct administrative review of access privileges based on function of new classification; remove access privileges that are not needed for new classification	conduct administrative and security review of access privileges based on function of new classification; enable access based on outcome of review	based upon administrative and security review; remove access privileges that are not needed for new classification	previous and new supervisors and/or department heads; or system owner	Previous and new IT managers and resource owners
	Employee	Classification Change (promotion, transfer, demotion, etc.)	external department	disable all access	none	permanent	previous and new supervisors and/or department heads; or system owner	Previous and new IT managers and resource owners
	Employee	Retirement	permanent	disable all access	none	permanent	supervisor and/or department head; or system owner	IT manager or resource owner
	Employee	Leave-of-Absence, Administrative Leave	internal department	conduct administrative review of access privileges based on nature of absence	conduct administrative and security review of access needs based on function of position; enable access based on outcome of review	based upon administrative and security review	supervisor and/or department head; or system owner	IT manager or resource owner
	Employee	Modified Service, Other Types of Service	internal department	conduct administrative review of access privileges based on function; remove access privileges that are not needed for function	conduct administrative and security review of access needs based on function of position; enable access based on outcome of review	based upon administrative and security review	supervisor and/or department head; or system owner	IT manager or resource owner
	Person-of-Interest	non-employee, contractor, consultant, guest, visiting scholar, vendor	legal contract or written agreement required between institution and person-of-Interest required	conduct administrative review of access privileges based contract or written agreement; remove access privileges when agreement expires or terminates	conduct administrative and security review of access privileges based contract or written agreement; enable access based on requirements of contract or written agreement	per contract or written agreement between institution and person-of-interest; remove all access privileges when agreement expires or terminates.	supervisor and/or department head	IT manager; ITSS Information Security; information owner(s); resource manager
	Supervisor or Department Head	Employee Absence or Termination	request for access to employee files; requester is supervisor of employee	conduct administrative review of access privileges based on employee function; remove access privileges that are not needed for employee function	conduct administrative and security review of access needs based on function of position; enable access based on outcome of review	30 or 60 day access based on administrative and security review	supervisor and/or department head	ITSS Information Security; information owner(s); system owner(s); resource owner(s); resource manager
Definitions								
resource manager								

Standards for Granting and Removing Access to Information Resources:
Guide for Departments

Service	User Type	Employment Status	Position Information	Action to be Taken	Minimum Access to be Enabled	Duration	Initiator/Requester	Service Provider(s) and Approver(s)
resource owner								
service provider								
initiator								
duration								
minimum access to be retained								
action to be taken								
position information								
employment status								
EIS ACES								
IT manager								
supervisor								
department head								
new hire								
termination								
classification change								
retirement								
leave-of-absence								
administrative leave								
modified services								
ITSS Security functions- may request, enable, or disable access for all user types								