

**ASTRA SECURITY AUTHORIZATION FORM**

**THE UNIVERSITY OF UTAH**

➤ Is this access intended to replace another employee's access that should be discontinued?  YES  NO If yes, who: \_\_\_\_\_

Applicant Name: \_\_\_\_\_

UID: \_\_\_\_\_ Email: \_\_\_\_\_

Office Phone: \_\_\_\_\_ Dept & Position: \_\_\_\_\_

Supervisor Name: \_\_\_\_\_ Supervisor Phone: \_\_\_\_\_

Supervisor Signature: \_\_\_\_\_

PRIVACY REGULATIONS: See the University of Utah Regulations, **Policy 4-001: University Institutional Data Management Policy** (available at: <http://www.regulations.utah.edu/it/4-001.html>)

Yes, I have read and will comply with the provisions for security and confidentiality of student records and files as described below. I also certify that I am a school official with legitimate educational interest in the records as defined in the Privacy Regulations. I understand that in accordance with the University of Utah Regulations, **Policy 5-111: Corrective Action and Termination Policy for Staff Employees** (<http://www.regulations.utah.edu/humanResources/5-111.html>), I can be disciplined and/or dismissed from employment if found to be in violation of this agreement.

I will:

- Access, distribute, and share student data, including test data, only as needed to conduct University business as specified in my position description.
- Respect the confidentiality and privacy of individuals whose records or data I access.
- Observe any ethical restrictions that apply to data to which I have access.
- Protect my security authorizations (user ID(s) and password(s)) and be personally accountable for all work performed under my security authorization.
- Protect confidential information displayed on my workstation monitor.
- Report knowledge of security breaches.
- Comply with all department and University security policies and procedures.

I will not:

- Discuss verbally or distribute in electronic or printed formats confidential student data except as needed to conduct University business as specified in my position description.
- Knowingly falsely identify myself.
- Gain or attempt to gain unauthorized access to student data or University computing systems.
- Share my user ID(s) and password(s) with anyone.
- Leave my workstation unattended or unsecured while logged-in to University computing systems.
- Use or knowingly allow other persons to use student data for personal gain.
- Make unauthorized copies of student data.
- Engage in any activity that could compromise the security or stability of student data.

Applicant Signature: \_\_\_\_\_

Date: \_\_\_\_\_

USER ACCESS: Which profile are you requesting?				
<input type="checkbox"/> APPLIED SCIENCE	<input type="checkbox"/> EHSEB	<input type="checkbox"/> HPR	<input type="checkbox"/> REPORTING	<input type="checkbox"/> OTHER:
<input type="checkbox"/> ARCH	<input type="checkbox"/> FMPH	<input type="checkbox"/> ITS	<input type="checkbox"/> SAEC	
<input type="checkbox"/> CMES	<input type="checkbox"/> GARFF	<input type="checkbox"/> NURS	<input type="checkbox"/> SFEBB	
<input type="checkbox"/> CSBS COMP	<input type="checkbox"/> GC	<input type="checkbox"/> PUB SAFETY	<input type="checkbox"/> SFESOM	
<input type="checkbox"/> CSC	<input type="checkbox"/> HPEB	<input type="checkbox"/> RAB	<input type="checkbox"/> UCL	

Security Coordinator Signature:

Authorized Scheduling Signature:

\_\_\_\_\_  
 Jessica Novak

\_\_\_\_\_  
 Elizabeth Johnson

Astra ID:

Date Access Granted:

Role(s) Granted: