New Mexico State University
Administration and Finance

A & F New Employee Form

ROUTING
FSA, MSC 3FSA
BFHRtech@nmsu.edu
Phone 646-6727
Fax 646-1994

Instructions: Type or print information. Complete one form per new employee. Fill in all applicable sections. Scan completed form and save file to the appropriate folder (AF, FS, or HR) on the ear$ drive. If assistance is needed to complete the form, please contact us at 646-TECH (8324).

SECTION 1: (Must be completed) REQUESTOR INFORMATION

Requester Name: _____ Requestor Title: _____

Phone: _____ Email: _____

Work Order: _____ Date Required: _____
(You will have a WO only if you notified FSA during the hiring process)

SECTION 2: (Must be completed) EMPLOYEE INFORMATION

Employee Type: ☐ Regular ☐ Temp ☐ Student ☐ FS Shop Employee ☐ Part time

Employee Name: _____ Aggie ID: _____

NMSU Email: _____ Supervisor: _____

Employee Title: _____ Department/Sub Dept Name: _____

This position is (check one): ☐ New Position ☐ Replacement of existing position

Previous Employee: _____

Special Software Requests: (Applications outside of the standard A&F software will need to be reviewed and authorized prior to installation)

_____

_____

List Shared folder access required on the A&F servers: _____

_____

_____

SECTION 3: (Must Be Completed) AUTHORIZED APPROVALS

Print Name: _____ Signature: _____ Date: _____

Reset Form

New Mexico State University Non-Disclosure Statement

This Non-Disclosure Agreement is intended to define the responsibilities of those employees who have access to the NMSU records that contain sensitive or confidential information about students, employees, donors, or other individuals, and to record his or recognition and acceptance of that responsibility.

New Mexico State University maintains the confidentiality and security of records in compliance with the Family Educational Rights and Privacy Act of 1974 (FERPA), the Health Insurance Portability and Accountability Act (HIPAA) and the Gramm-Leach-Bliley Act (GLBA), in addition to other federal and state laws. These laws pertain to the security and privacy of personal academic, medical and financial information, along with identifying information such as social security numbers.

FERPA protects student records. FERPA requires post-secondary educational institutions and agencies to conform to fair information practices in their handling of student data. Among the provisions of the act are the requirements that data be used only for intended purposes and that those responsible for student data take reasonable precautions to prevent misuse of it. Examples include Social Security Numbers, grades, date of birth, etc.

HIPAA protects all medical records and other individually identifiable health information used or disclosed in any form, whether electronically, on paper or orally.

GLBA protects private, non-public, information of individuals. Private, non-public information consists of information such as name, Social Security Number, date, and location of birth, gender, credit card numbers, and driver's license numbers.

Within NMSU, employees are authorized access to University records only to the extent necessary to perform their official university duties, and are responsible for protecting such information against unauthorized access or disclosure.

Employee: Recognizing this responsibility, I agree to the following (please initial each line):

_____I will access university records only as required to perform my assigned duties.

_____I will not access student employee information this is not necessary to carry out my job. This includes the records of my children, my souse, significant other, parents, other relatives, friends, and acquaintances.

_____I will store information under secure conditions and make every effort to ensure individual's privacy.

_____I will not divulge, copy, release, sell, loan, review, alter, or destroy records except as properly authorized by the appropriate university official within the scope of applicable state or federal laws, record retentions schedules, and internal policies.

_____I will forward all requests for information via an open records request to the university's General Counsel for guidance. I will not release information covered by these requests until instructed to by university's General Counsel or my supervisor.

_____When I release student information, I will divulge only the information regarded as "directory" or public information, specifically the student's name, address, telephone listing, date and place of birth, major field of study, classification, participation in any officially recognized activities and sports, eight or height of members of athletic teams, dates of attendance, degrees and award received, and most previous educational institution attended.

_____I will not release any information about a student who has requested a total suppression of information nor will I release any optional directory information on an employee who has requested to have his/her directory information suppressed.

_____I will not release information about students, staff, or employees that was requested on the basis of non-public information (for example-names of all international students, names of all students with a GPA of less than 2.0 etc.)

_____I have read the NMSU Non-Disclosure Agreement and agree to comply with its provisions. I understand that failure to comply may result in disciplinary action, including termination of employment.

Print Name_____Employee Signature/Date _____

COMPUTER & MOBILE DEVICE USE GUIDELINES

Updated 8/1/2016

These policies and guidelines are derived from the NMSU Policy Manual and ICT's Security, Policies and Guidelines (#2.35)

- Computing and Mobile Device equipment, and associated resources, are owned and administered by the Board of Regents of New Mexico State University. Access to this equipment is a privilege granted to students and employees to facilitate instruction, research and administration. University equipment is intended for work use only.
- The use of University resources for support of private enterprise such as outside consulting should only be in accordance with stated policies, and under explicit written agreements.
- Use of the system to send or view fraudulent, harassing, obscene, indecent, pornographic, intimidating or unlawful communications is prohibited.

Employees downloading, printing, accessing, forwarding, transmitting or viewing pornographic material on the university computers during and after work time is not allowed. Those who may happen to see the material could potentially report the incidents as offensive and/or inappropriate for the work environment.

- University employees will report lost or stolen equipment immediately.
  - User reports the loss to their supervisor and to FSA.
  - For mobile devices, the User and FSA will make a concerted effort to locate the equipment.
    - The User should revisit all locations they were at and ask building monitors and occupants if the device has been turned in.
    - The User should ask coworkers if they remember seeing the device.
    - FSA will monitor the network for 2 weeks to see if the device has communicated with the MDM software and, if so, attempt to determine the location of the device.
    - If the device has not been found at the end of 2 weeks, FSA will work with the User's department to purchase a replacement.
- University employees shall not download or upload unauthorized software over the internet.
- University employees shall not copy licensed software.
- University employees shall use licensed software in accordance with the license agreements.
- The users of the computing resources are expected to take a responsible and professional approach to the use of those resources. Since the resources are shared, everyone must accept responsibility of minimizing the impact of one's actions on others.
- The university and its departments shall grant accounts for access to university computer resources. The holder of an account will be held responsible for activity on that account. Account holders should change passwords frequently and should not reveal their passwords to anyone
- It is a violation of university policy for employees to share user accounts and passwords.
- The university has specific permission to inspect client's accounts and files space for possible violation of University policy. This includes email.
- Certain accounts on PC's called administrator accounts have full control over security and software installation on the PC. Users with this type of account should take extra precautions to safeguard university resources. No unauthorized software or hardware should be installed.

All users of NMSU computing and mobile device equipment and resources are required to affirm the following:

I have read the above policy and guidelines, and I understand and agree to abide by the terms of the policy. I also understand that my use of NMSU equipment and resources must be in accordance with the policy. I recognize that violations of this policy may cause restriction or elimination of my access to NMSU computer resources, other disciplinary action, or civil or criminal penalties.

Printed Name	Aggie ID
Signature	Date