Access Control Policy

PREPARED BY	**ORGANIZATION**	**DATE**
Wade Craig and Patrick Murphy	NRAO	May 5, 2020

APPROVALS (Name and Signature)	**ORGANIZATION**	**DATE**
Tony Beasley	NRAO	September 30, 2020

Change Record

VERSION	DATE	REASON
1.0	May 5, 2020	Release Candidate

ACCESS CONTROL POLICY

(FORMERLY: SYSTEM/NETWORK ADMINISTRATION SECURITY PRACTICES)

1 INTRODUCTION

Access control is fundamental to information security and represents the organization's policies and practices around who has access to what information and information systems, the extent of that access (i.e., level of privilege), and when and under what conditions that access is granted and revoked.

This document is a high level statement of the Observatory's mandatory access control policies and core procedures.

Except where clearly indicated by wording such as "recommended" or "should", all practices described in this appendix are considered to be mandatory. These required practices are intended to establish the minimum level of security across the NRAO; stronger security measures may be implemented provided that they are approved by the Information Security Office and that they do not interfere with compliant operations at any site.

2 NETWORK SERVICES

- Services provided by an NRAO site which are accessible from the Public Internet must be approved by the Information Security Officer/Computing Security Committee.
- Each site will have at least one firewall. The firewall(s) will control all access between public Internet and all internal Observatory resources.
    a. When an approved service is available externally, a firewall must permit such access only to the systems which provide the service, and only from the class of network which requires it.
    b. Services which are not required outside of a site must be blocked by a firewall from all external access.
- Any equipment which provides services available outside of the LAN must use software which can be configured to refine access control.
- Systems providing any service that runs on an operating system which has reached an End of Support status must be situated on a private network, with no direct access to or from the Public Internet. In addition, such systems must restrict any login accounts to the minimum needed for operation thereof. NRAO managed, up to date operating systems, with all relevant security patches applied.
- Systems providing any service that run on a non-current operating system must be situated on a private network, with no direct access to or from the internet at large. In addition, such systems must restrict any login accounts to the minimum needed for operation thereof.
- Any system offering a service that does not comply with the above rules and, for operational reasons must be accessed from outside NRAO networks, must have its network access restricted to only

necessary network ranges. Such exceptions must be reported to, and documented by, the Information Security Officer and the NRAO Network Manager.

- Network login access to a system which cannot support modern authentication mechanisms may originate only from the LAN.
- Terminal/access servers attached to an NRAO network must require encrypted user account and password verification.
- Filters for electronic mail delivery which are applied at the system (not individual user) level to reduce nuisance messages must be approved by the Information Security Office; complaints to external organizations regarding such activity must first be approved by the Information Security Office.
- Services which require the transmission of sensitive data such as account passwords, and which cannot support secure connections (e.g. by use of encryption) must:
    1. Be approved by a member of the Information Security Office;
    2. Be disabled; or
    3. Use a proxy server/portal system; or
    4. Be restricted to systems on which the service is absolutely required, or which provide no other services.
- Visitors wishing to connect devices to NRAO's networking infrastructure must automatically receive network services that place their systems on a special "visitor" network (eg: Guest WiFi or Guest Wired Network). These visitor networks will have no more privilege to access NRAO internal resources than any user from the internet.

3 ACCOUNTS

- Access to NRAO computer facilities will be granted only to NRAO/AUI employees and others (including, but not limited to, scientific visitors) approved by the site Assistant Director or IT Site Manager. Only authorized system administrators may grant access to an NRAO computer account.
- Access by authorized system administrators to accounts other than their own will be only when necessary in the course of normal technical duties. System administrators are obligated to maintain and protect the confidentiality of any information accessed in this manner, except where violations of NRAO policy or the law are uncovered in the course of their work.
- Access by users other than authorized system administrators to another user's account (as defined above) for legitimate work-related reasons will only be granted with written approval from the supervisor of the user granted access and the supervisor responsible for the accessed account. Furthermore, copies of such approval must be delivered to the Information Security Officer and the Site Human Resources Manager before any work is performed.
- All access to NRAO computer accounts, whether originating on-site or elsewhere, requires an initial password or passphrase challenge that is verified by an NRAO system. Secure web access using SSL (https), VPN connections, and software such as the secure shell (e.g.: ssh, sftp, putty), all of which encrypt the authenticating information in transit, are acceptable.
- Access to privileged accounts from outside of NRAO, whether direct or by using another account first, is only permitted via encrypted connections.

- Interactive login access to service available outside the NRAO via the Public Internet is to be permitted only to site login servers and other approved bastion hosts (as defined in the Master Information Security Policy).
- Access to systems via a privileged account that does not require a password challenge may originate only from a secure internal server, whether or not an encrypted connection is used. Only privileged, administrative, and system accounts are permitted to login to primary servers and bastion hosts.
- Passwords may not be stored in unencrypted computer files for the purpose of eliminating a password challenge. Secure key or token-based access is permitted.
- A password or passphrase challenge is mandatory when an escalation of privilege or change in identity occurs, e.g. the use of the "su" command to change UID. Any ssh key used for access to a different account must be encrypted.
- Administrative and Privileged accounts will be granted to users who are not authorized system administrators only if the normal function of their duties requires such access. This must be communicated to the Information Security Office.
- Unless the platform type does not support it, user accounts will be disabled after 10 consecutive failed logon attempts to a system.
- Guest accounts should be disabled when the term of use has elapsed. Other accounts should be disabled after 3 months of inactivity.

4 REMOTE ACCESS

Remote access is the circumstance where an authorized user is establishing a connection to an NRAO system or network from a location that is not under the NRAO's control. This includes, but is not limited to, interactive login sessions, file transfer, and accessing electronic mail.

- Remote access services and servers hosted by the NRAO must be approved by the Information Security Office.
- All interactive connections (including but not limited to ssh and ftp) must be presented with the following banner before login:

```
National Radio Astronomy Observatory computing facilities
 are exclusively for the use of authorized personnel, who
  are expected to abide by all applicable NRAO Policies.
```

- Access via public Internet/Intranet
  - Use of VPN (Virtual Private Network) technology from an Observatory-owned computer to access internal Observatory resources is preferred.
  - Where VPN is unavailable, the connection must be established using a protocol that uses encryption to protect passwords and other sensitive information.

5 INTERNET FACING SERVERS AND SERVICES

Internet-facing protocols and applications require special precautions because of the potential for security breaches unique to them.

- Only authorized Observatory system administrators may install servers and services which are accessible from the public Internet.
- Servers that provide services accessible to the public Internet without restrictions may also provide other services externally, but these must be limited to related information services.
- Specialized servers, i.e., those installed for specific internet-facing uses by specific users or groups, must restrict external access, preferably via an authenticated connection. If traditional encryption or authentication techniques are not possible, access must either require the use of a password or be restricted to specific remote IP numbers and approved by the Information Security Office.
- All Internet-facing devices and servers must maintain a reasonable patch level with respect to Operating System, necessary software and related hardware/firmware updates. All critical updates must be addressed in a timely manner.
- The implementation and deployment of web services will be monitored and controlled. Only authorized system administrators or identified developers in conjunction with a system administrator may install active web-facing applications on externally facing servers. All applications receiving input from users of the Internet must check and sanitize input parameters before further processing.
- All publicly facing devices and systems, including applications, will be routinely scanned for vulnerabilities.
- All publicly facing devices and systems must be segregated from internal Observatory resources.
- Storage of sensitive data on any server must comply with the NRAO Data Security Policy and Data Privacy Policy.

6 INTRUSION DETECTION

The requirements of this section apply to non-NRAO equipment that is located on NRAO premises for a period of over 3 months.

a. Logging

- All access-logging facilities supported by operating systems and service-related application software will be enabled on all systems, including terminal/access servers, firewalls, and network-perimeter devices. Exact level of auditing to be determined on a per-system basis as recommended by the Information Security Office in conjunction with Observatory System Administrators.
- Alarm and alert functions will be enabled on firewalls and other network-perimeter devices.
- Where supported, log entries will be written to a central facility on a secure internal server to preserve integrity and facilitate examination.
- Where supported, failed authentication attempts must be recorded in an audit log for later inspection and action, as necessary.

- Log files must be readable only by privileged/administrative accounts unless other access is required for proper functioning of an application.
- Weekly backups of logs must be made and stored offline.
- Log entries from access control systems, servers, and other LAN hosts will be reviewed as necessary. Reviews may include examination for hostile and aggressive activities as well as intrusion attempts.

b. Checks

- System integrity checks of firewalls, access-control systems, and any system which provides services outside of the LAN should be performed regularly using techniques such as checksums on files or comparison of current files against trusted backup copies. Periodic checks are recommended for all other systems as well.
- Anti-virus tools will be used to scan every endpoint as well as servers for which malware are a known hazard. These tools, as well as their pattern/definition files, must be kept current.
- All Observatory systems will be monitored for indicators of compromise (including, but not limited to, indications of intrusive activity). Suspicious symptoms must be reported promptly to the Site Security Group.
- The Information Security Office will routinely scan all systems both internally and externally (aka: "on the LAN and on the WAN"), to check for security-related patches issued by operating-system and application software vendors, work with System Administrators to ensure that such patches are applied as promptly as possible, and to monitor compliance.

7 PASSWORDS, PASSPHRASES AND SSH KEYS

- All account passwords are chosen in compliance with the NRAO password guidelines at https://info.nrao.edu/computing/guide/passphrases-passwords. The NRAO Computing Security Committee will regularly review the guidelines and revise them as necessary.
- Passwords will be disclosed only where absolutely required to perform one's duties—as a rule, an Observatory account password should never be shared.
- Periodic password evaluations may be conducted to ensure that passwords are reasonably secure. Any password which is uncovered during an evaluation must be changed within 2 business days after the account user is notified.
- Any password which is suspected to have been compromised will be disabled and must be changed immediately. Additionally, passwords must be changed when:
    1. An employee with knowledge of privileged account passwords either leaves the Observatory's employ or otherwise ceases to be responsible for tasks which require them; or,
    2. The password has been given to an outside party for diagnostic/support purposes and the service is complete.
- Privileged and administrative account passwords must be different on different classes of systems and platform types. An annual change is required.
- System accounts must be used only for controlling services, and will be disabled for interactive use.

- Guest account passwords must be changed at least when the account is reassigned, and the account must be disabled when not in use.
- All shared accounts must be disclosed to, and approved by, the Information Security Office. Shared account passwords must be changed annually.
- Administrative account passwords and passphrases used to secure SSH keys granting root level access are to be changed annually. Private SSH keys are not permitted to be shared.