University of Arkansas at Little Rock (UALR) Network and Access Guidelines

University of Arkansas at Little Rock (UALR) infrastructure including but not limited to wired and wireless connections, all of the devices and component are used to provide access to UALR services, servers, systems, data and internet resources.

These guidelines define general principals about network and access management.

Scope

These guidelines can be used by UALR users, including but not limited to students, faculty, staff, contractors, guest and systems, servers, data, infrastructure and infrastructure components.

1.1.1 Any user should follow the access provisioning procedure to request access to systems, servers, infrastructure or data.

1.1.2 All un-necessary, un-used identities and access rights should be removed.

1.1.3 If any of the user has system or services management responsibility other than a user level responsibility, a unique management identifier must be assigned.

1.1.4 Privileged access is managed by centrally managed Active Directory system.

1.1.5 If a system cannot be managed by Active Directory system, an exception must be defined and IT Services ISO must approve the exception.

1.1.6 Access to system APIs or other means of viewing transactional data, making modifications to program logic or other enhancements to centrally managed applications is strictly limited to authorized personnel within IT Services. Request for access may be made to the CIO or designee. Request for access does not imply approval. Appeals on denials may go to the VC Finance and Administration.

1.1.7 All types of local management passwords on network devices or components must be kept in a secure encrypted form.

1.1.8 Management passwords provided by the vendor and default passwords must be changed immediately and the new password must comply with UALR Password Policy

1.1.9 The owner is accountable for the access requests. The owner can approve or reject the requests.

1.1.10 Standard access rights will be removed immediately after of departure from UALR. IT Services will be notified of departures via (we need a procedure)

1.1.11 Elevated access rights will be removed immediately upon notice of departure.

1.1.12 Removal of access rights may be requested of persons with in a division by the Dean, AVC or VC of the division ….

1.1.13 Student accounts may be revoked in cases involving

1.1.13.1 Departure from UALR

1.1.13.2 Upon notice from the Provost or AVP of student affairs.

1.1.14 All role changes must be reviewed and roles no longer necessary to perform new responsibilities may be revoked.

1.1.15 Since application source codes provide a lot of details and insights about applications, source codes should also be protected and access to sources must be limited to authorized developers and/ or users.

1.1.16 Development systems, servers and services must be isolated from other services, servers and systems, specifically from production environment. Production services, servers, system and application can not store, host or run source codes or source code developments systems.

1.1.17 Access to source codes should be restricted and should be logged.

1.1.18 IT Services Technology, Infrastructure and Operations Director enables and applies all of the required security features and components to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks and to protect the connected systems and applications, including open ports, access to web portals and applications. Moreover, network should be implemented and configured such a way to maintain the availability of the network services

1.1.19 [REVIEW]Privileged access rights should be assigned to a user ID different from those used for regular business activities. Regular business activities cannot be performed from privileged ID and privileged activities cannot be performed with regular user IDs.

1.1.20 All of the activities of the users who have privileged access must be logged and these logs must be kept for at least 3 moths.

1.1.21 These privileged activities must be monitored and reviewed. Since logged data will be huge, if UALR has not the necessary systems to review the logs automatically, a manual review may be performed. However, it will not be effective and the amount of logged data is very big, review process can be skipped. In this case, logged data should be kept at least for 1 year.

1.1.22 All privileged access owners should be informed about logging, auditing processes.

1.1.23 Privileged access rights must be reviewed at least once a year and un-used accounts or un-necessary accesses must be revoked.

1.1.24 Data classification procedure should define the rules and requirements to access to data. Based on the classification of data, access rights must define user's right to read, write, delete and execute the data or applications.

1.1.25 If a service, systems, infrastructure or application have access to another one, access right must be defined based on "need-to-know" and "least-privilege" principals.

1.1.26 If a service, system, infrastructure component or application provide an output for other service, system, infrastructure component or application, the output should contain only the necessary information necessary to perform the expected function. Therefore, the output must be restricted and formatted accordingly.

1.1.27 The security level for services, systems, infrastructure components, data and applications containing business critical and sensitive or secret information, application or service must be set to highest level and they must be isolated from other services, systems, infrastructure, data and applications which have lower level security. A protection system including but not limited to firewalls, infrastructure segmentation, active protection and intrusion prevention systems must be implemented.

1.1.28 In order to protect business critical and sensitive systems, services, infrastructure, application and data, the following safeguards must be implemented:

1.1.28.1 No system, application or data identifier must be displayed until the log-on process has been successfully completed;

1.1.28.2 No help message, no password recovery clue must be provided during the log-on procedure that would aid an unauthorized user;

1.1.28.3 Log-on information must be validated only on completion of all input data. If an error condition arises, the system should not indicate which part of the data is correct or incorrect. It must be prohibited to use any message showing which part of the information is wrong. Therefore, only “Can not logon”, “information is incorrect”, “credentials can not be validated” type of error messages must be used;

1.1.28.4 In order to prevent brute force attacks, number of un-successful access request must be limited to at most 5.

1.1.28.5 All successful and un-successful access attempts must be logged and the records should be kept at least 3 months.

1.1.28.6 If log-on process is successful, user should see date and time of the previous successful log-on, details of any unsuccessful log-on attempts since the last successful log-on;

1.1.29 Inactive sessions should be terminated after 15 minutes of inactivity.

1.1.30 Network installation, configuration and operation procedures should be documented and should be kept updated on document management servers

1.1.31 Mobile units should be protected using adequate security measures.

1.2 Network Security Management

1.2.1 Security of Network Services

1.2.1.1 Network devices and components use TACACS+ to authenticate networks managers.

1.2.1.2 Technology, Infrastructure and Operations Directorate may prefer to create a local management account on network devices to provide service continuity and to perform incident management processes.

1.2.1.2.1 Local accounts must be configured to be highly secure. Local accounts must be encrypted and all of the activities of management accounts must be logged and the records must be stored at least for 1 year.

1.2.1.3 The following services or features must be disabled on all network devices or components :

1. IP directed broadcasts
2. Incoming packets at the router/switch sourced with invalid addresses such as RFC1918 addresses
3. TCP small services
4. UDP small services
5. All web services running on router
6. Cisco discovery protocol on Internet connected interfaces
7. Telnet, FTP, and HTTP services
8. Auto-configuration

1.2.1.4 The following services should be disabled unless a business justification is provided:

1. Discovery protocols
2. Dynamic trunking
3. Scripting environments, such as the TCL shell

1.2.1.5 The following services must be configured:

1. Password-encryption
2. NTP configured to UALR standard source

1.2.1.6 All routing updates must be done using secure routing updates. Routing updates must be exchanged via encrypted and authenticated communication links.

1.2.1.7 Customized UALR SNMP community string must be used. Default strings, such as “public” or “private” must be removed.

1.2.1.8 SNMP must be configured to use the most secure version of the protocol allowed for by the combination of the device and management systems.

1.2.1.9 Access control lists must be used to limit the source and type of traffic that can terminate on the device itself.

1.2.1.10 Access control lists for transiting the device are to be added as business needs arise.

1.2.1.11 The router must be included in the corporate enterprise management system with a designated point of contact.

1.2.1.12 Each router must have the following statement presented for all forms of login whether remote or local:

> *"UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED. You must have explicit permission to access or configure this device. All activities performed on this device may be logged, and violations of this policy may result in disciplinary action, and may be reported to law enforcement. There is no right to privacy on this device. Use of this system shall constitute consent to monitoring."*

1.2.1.13 Telnet should never be used across any network to manage a network device or component, unless there is a secure tunnel protecting the entire communication path. Latest version of SSH is the preferred management protocol.

1.2.1.14 IT Services has the authority to install, to remove any network devices or to change their locations, to add or remove services running on network devices or components and to apply or to remove access restrictions on network devices and components based on business requirements and educational requirements.

1.2.1.15 In order to provide a more secure computing environment, to keep confidentiality of UALR business critical and sensitive data and to mitigate the negative effects of malicious attacks, UALR rely on segregation in infrastructure, services and systems.

1.2.1.16 Segregation should be implemented based on trust levels, business functions, “need-to-know” and “least-privilege” principals. Both physical and logical segregation should be considered and implemented.

1.2.1.17 The perimeter of each domain should be well defined. Access between segregated domains may be allowed, but should be controlled at the perimeter using a gateway (e.g. firewall, filtering router). The criteria for segregation of networks into domains, and the access allowed through the gateways, should be based on an assessment of the security requirements of each domain. The assessment should be in accordance with the access control policy, access requirements, value and classification of information processed and also take account of the relative cost and performance impact of incorporating suitable gateway technology.

1.2.1.18 Wireless networks require special treatment due to the poorly defined network perimeter. All wireless access should be considered as external connections and to segregate this access from internal wired networks until the access has passed through a gateway.

1.2.1.19 All of wireless access devices and components must apply authentication, encryption and user level network access controls