Policy on Network and Systems Administration

MICHIGAN
ROSS SCHOOL OF BUSINESS

Purpose

The Stephen M. Ross School of Business at the University of Michigan (“Ross”) outlines responsibilities, guidelines and standards of conduct for all individuals who function as network or systems administrators. Network and Systems Administrator (“Administrators”) are individuals who perform any network/system administration duties and/or technical support of network/systems that are accessed by other people, systems, or services. Administrators represent the shared interests of Ross and the entire University of Michigan community in informing and protecting on all appropriate matters pertinent to their responsibilities.

Guiding Principles of the Network and Systems Team

- Fast-paced environment; Often quick adoption required.
- Leading edge technologies; Often set the pace of campus.
- High rate of change; High financial commitment from the Dean.
- Protect confidential and private data through leading edge security methods.
- High expectations for reliability and customer service; Outages must be rare and brief.
- Equal partners with the HelpDesk team.
- Operate more like a business than a University; Well-defined processes; Accurate and realistic project planning; Accurate timelines; Expectation of a corporate IT model.

Network and Systems Administrator Responsibilities

As part of normal business processes and practices, Network Administrators are:

- Held to the highest standard of behavior and ethics because they have the capability and responsibility to maintain system integrity and must be trusted with the security and privacy of all data on the network.
- Allowed access to users' private information and, as such, are required to protect the privacy, confidentiality and integrity of this information at all times.
- Expected to take every reasonable effort to safeguard services and data stored on the Ross network. Administrators are not liable for any loss of data or loss of service on the Ross network. The ultimate responsibility for safeguarding data rests with the user through proper security and archival procedures.
- Required to notify appropriate UM departments and their supervisors of any observed violations of University computing policies, licensing agreements with software manufacturers, or observed violations of local, state, or federal laws regarding these matters.
- Charged with investigating policy violations and suspected abuse of computing resources. Where violations of a policy occur, Administrators are authorized to take reasonable actions to implement and enforce the usage and service policies of the system and to provide for security of the system. During such investigations, Administrators may inspect any data files and may monitor network traffic.
- Required to follow the Ross Policy on Security Incident Response
- Follow additional responsibilities to the University as a whole, regardless of the policies of Ross and Computing Services.

Best Practices

The following best practices will be followed as part of normal business processes and practices:

- Disaster recovery plans of critical systems and services will be developed and reviewed on an annual basis. All administrators will become familiar with the plan. Key systems and services will be tested against the disaster plan on a regular basis as determined by the Administrators. A copy of the plan will be stored on the department SharePoint site and a backup copy will be stored securely offsite.
- File and data backup plans will be kept and followed for all systems and services.
- Backup media will be stored off-site to minimize risk. All media will be rotated and destroyed on a regular basis.
- All system passwords will be changed on an annual basis. Safe password guidelines will be followed at all times.
- Log files on critical systems will be reviewed regularly for possible intrusion detection. Automated processes will be developed and used whenever possible in order to filter out actual abuses and to keep the review window as short as possible, ideally every day.
- Administrators will never authenticate to critical devices or services with administrative rights when performing non-administrative tasks.
- All network and systems changes, no matter how trivial the change may appear, will go through a written peer review process with change logs that includes a plan for migrating development environments into production environments. Planning must include ensuring that data is safely transferred without loss or breach.
- Critical systems and Ross specific settings will be documents as required (see Network and Systems Documentation).
- Every attempt will be made to adopt the latest advances in security hardware, software and methods that do not interfere or restrict the teaching, learning and research mission of the Ross School or it's community of faculty, staff, students and alumni.
- Permission must be obtained from department heads before access to sensitive data is granted to any Ross person outside of the department that owns the data.
- Maintain the application software in a fully supported version with all appropriate patches and updates.
- Configure and maintain the systems, software and end-user computers in a way that optimizes security.

Job Related Duties

Administrators will use reasonable efforts to:

- Take precautions against theft of or damage to the system components.
- Faithfully comply with the terms of all hardware and software licensing agreements.
- Become familiar with all applicable Ross and University of Michigan policies.
- Participate in required Administrator training and regular campus meetings as necessary.
- Cooperate with Administrators across campus to implement new services or security methods, to install new features of existing services, to find and correct problems caused on another system by the use of the system under his/her control.

Network and Systems Documentation

Administrators shall create, maintain and update documentation of all network and systems that attach to the University network. Purposes are: Identify all systems in such a way that they can be understood by causal to advanced readers; help resolve all outages in a timely manner; provide highly available systems and consistent service delivery; and proactively maintain, monitor and support the entire Ross technology environment. This documentation will reside on SharePoint and is the foundation for Disaster Recovery Planning.

The report must include the following information:

1. Logical diagrams of all Ross technology networks and systems
2. Physical diagrams that correspond with each logical diagram
3. Systems configurations for each of the physical components that include:

    - Manufacturer, model and serial number.
    - Operating System and revision number.
    - IP and MAC address of all network interface cards within the system.
    - Computer's host name(s) and primary user's information.
    - Physical location of the equipment.
    - Detailed description of the service provided.
    - Identification of the Ross departments, constituents or owner of the service.
    - System's primary functions (e.g. web services, file server, mail server, personal computer, etc.).
    - Special installation and configuration settings, parameters, patches, devices, etc. that are unique or required for the Ross environment.

4. Server room rack diagrams and locations for each physical component.