Guidelines on Appropriate Use of Administrator Access to Information Resources

Approving authority	Information Security Steering Committee
Approval date	26 March 2014
Advisor	Bruce Scott | Director ITI, Information Services b.scott@griffith.edu.au | (07) 373 57468
Next scheduled review	2019
Document URL	http://policies.griffith.edu.au/pdf/Guidelines-on-Appropriate-Use-of-Administrator-Access-to-Information-Resources.pdf
TRIM document	2014/0006767
Description	The purpose of this guideline is to instruct users on appropriate use of Administrator Access to University computing and information resources.

Related documents

Code of Conduct
Griffith University Privacy Plan
Information Technology Code of Practice
Student Misconduct Policy
Information Security Policy
Information Security Policy - Schedule A: Roles, Standards and Operational Procedures

1. INTRODUCTION

The University Information Security Policy places additional obligations on users with privileged or high-level access rights. These staff members are required to abide by the Code of Ethics promulgated by the System Administrators Guild of Australia. System Administrators found guilty of breaching this Code of Ethics may be subject to disciplinary action.

Granting of privileged or Administrator level access for production systems to other than specialist system administrators is an exception and comes with responsibility not only for the individual system but the wider health, security and integrity of the University's services, data and reputation.

2. GRANTING OF ADMINISTRATOR ACCESS

2.1 Principle of Least Privilege

University systems are operated on the principle of least privilege.

The principle means granting a user account only those privileges which are essential to the performance of that user's work. For example an account used for backing up a system would not be granted privileges to install software.

2.2 Alternatives to Administrator Access

Most operating systems and applications contain facilities that allow non-Administrator accounts to be granted permission to perform a defined set of functions that would normally require administrator access without granting full administrator access.

Such privileges can be granted for a defined period or on a continuing basis. Examples include the ability to start and stop applications, read system logs, reboot a server and alter application settings. When available these alternatives will be used in preference to administrator access.

2.3 Use for purpose given

Administrator access is only to be used for purposes for which it was granted. Administrator access does not imply authorisation to undertake activities that are enabled via the privileged access but are not within the purposes for which it was granted.

2.4 Process for granting administrator access

2.4.1 A request for administrator access will be submitted to the System Owner for approval. A request can include multiple systems.

2.4.2 The System Owner is the Director, Dean or Head of School/Department of the business area with responsibility for the system

2.4.3 The request must address

- Why requirements cannot be achieved by alternatives to administrator access
- The business reasons for access
- Identified risks and mitigations. (See 4.1)

2.4.4 Approved requests for access will be submitted to INS for action.

2.4.5 Requests will be reviewed for IT Security reasons and may be rejected if risks and mitigations are inadequate.

3. INAPPROPRIATE USE OF ADMINISTRATOR ACCESS

In addition to those activities deemed inappropriate in the University Code of Conduct and Information Security Policies, the following constitute inappropriate use of Administrator Access.

3.1 Inappropriate use of Administrator Access to University computing resources unless documented and approved by the System Owner

- Circumventing user access controls or any other formal University security controls
- Circumventing bandwidth limits or any other formal University computing controls
- Circumventing formal account activation or suspension procedures
- Circumventing formal account access change request procedures
- Circumventing backup process or other mechanisms designed to ensure the retention and integrity of University data
- Circumventing any other University policy
- Circumventing University change control procedures for IT systems.

3.2 Inappropriate use of Administrator Access to University computing resources under any circumstances

- Accessing non-public Information that is outside the scope of specific job responsibilities
- Exposing or otherwise disclosing non-public Information to unauthorized persons
- Using access to satisfy personal curiosity about an individual, system, practice, or other type of entity.

3.3 Personal use is not acceptable

- While the University Code of Conduct permits limited personal use of computing resources, this is restricted to **non-administrator** activities.

4. ADMINISTRATOR ACCESS BY THIRD PARTIES

Some applications are hosted on University infrastructure and supported by an external third party under contractual arrangements. In a limited number of cases support by the third party requires Administrator access. In addition to the requirements above the following guidelines must be followed.

4.1 Risks must be addressed

4.1.1 The System Owner is responsible for ensuring that the type of data on the system is identified and risks are identified, mitigated and recorded.

4.1.2 Particular area of concern are:

- Privacy related data in respect of Queensland and Federal Government Privacy Principles and any Privacy Act implications
- Staff, Student and Research data
- Data that has implications for ethics, confidentiality or intellectual property
- Third parties access, retention and disposal of data.

4.1.3 If the system interfaces with other University systems, the System Owner must also consider risks to these systems and their data.

4.1.4 Contractual arrangements with the third party should adequately address identified risks.

4.1.5 Risks and mitigations must be registered in the IT risk register and ownership of risk assigned.

4.2 Access will be via Virtual Private Network (VPN)

4.2.1 All access will be via the University VPN facility.

4.2.2 In accordance with the University security policy, one VPN account per person at the vendor end is required.

4.2.3 For vendors with a large number of support staff, a generic account may be issued.

4.2.4 When a generic account is provided, vendors must be able to identify on request who utilised the account from their organisation

4.2.5 VPN password must be changed every six months and must comply with University standards for composition and strength.

4.2.6 In the exceptional case where access cannot be achieved via VPN, access will be opened for the duration of the issue or incident only and use only approved access mechanisms.

4.3 Access Mechanisms

4.3.1 All access mechanisms will be via an encrypted service and utilise encryption mechanisms and strengths that match University standards.

4.3.2 Web-based administration must be via secure HTTP (HTTPS) and utilise a valid SSL certificate of not less than 2048 bits issued by a University certificate authority.

4.3.3 Webservers and applications will be configured to restrict access to administration services to specific IP addresses or address ranges that will be used to administer systems. Where address ranges are used they should be as narrow as possible.

4.3.4 Whenever possible administration services should be restricted to internal non-routable addresses.

4.3.5 Administrator access via unencrypted mechanisms such as telnet and ftp is prohibited.

4.3.6 Standard supported access mechanisms are SSH over VPN for Unix systems and RDP over VPN for Windows systems.

4.3.7 Direct login as root to Unix systems is prohibited.

4.3.8 Third party remote access tools will be considered on a case by case basis. The onus to prove suitability and security of third party tools is on the vendor.

4.3.9 Vendors are expressly prohibited from providing access to other parties.

4.4 External Access should be moderated

4.4.1 Wherever practicable the vendor's administrator account should only be enabled for the duration of required work or investigations and then disabled.

4.5 Network Controls

4.5.1 Systems which allow third party administrator access must be built and deployed such that access to other University services and systems is minimised.

4.5.2 An appropriate mix of network controls such as DMZ networks, intrusion detection and firewalls and network ACLS will be used.

4.6 Change Control

4.6.1 Change control will comply with University change control procedures for IT systems. This includes but is not limited to the change management process, authorisation by the Change Advisory Board (CAB) and IT architecture governance processes.

4.7 Operating System Configuration and logging

4.7.1 The operating system will be deployed, secured and configured in accordance with University standards.

4.7.2 Appliances or pre built virtual machines will be assessed by the University security and server support groups for hardening and security.

4.7.3 A copy of operating system and access logs will be made to a system the vendor cannot access. Wherever possible copying will occur in real time.

4.7.4 Operating systems will be patched in accordance with University guidelines.

4.8 Testing and vulnerability assessment before deployment

4.8.1 IT Security will perform a vulnerability scan of the server or service prior to it going live.

4.8.2 Vulnerabilities will be rectified or mitigated before going live. Where rectification or mitigation is not possible or practicable, a risk must be entered in the University IT risk register.