Contents

Section 1. Policy Overview................................................................. 1
  1.1 Policy statement........................................................................... 1
  1.2 Reason for the policy ................................................................. 1
  1.3 Primary guidance to which this policy responds ....................... 1
  1.4 Responsible college office and officer ...................................... 1
  1.5 Who is governed by this policy ............................................... 1
  1.6 Responsibilities ....................................................................... 1

Section 2. Policy Text........................................................................ 2
  2.1 Introduction ............................................................................... 2
  2.2 Default computer groups........................................................... 2
  2.3 Default administrator privileges .............................................. 3
  2.4 Request process ........................................................................ 4
  2.5 Appeal process ......................................................................... 4
  2.6 Approval duration .................................................................... 4
  2.7 Education requirements ......................................................... 4
  2.8 Privilege revocation .................................................................. 5

Section 3. Policy Reference.............................................................. 6
  3.1 Contacts .................................................................................... 6
  3.2 Cross reference to related policies .......................................... 6

Section 4. Glossary............................................................................ 7
  4.1 Definitions ................................................................................. 7

Section 5. Revision History.............................................................. 8
Section 1. Policy Overview

1.1 Policy statement
⇒ Administrator privileges allow a user to have full access of a local computer. Administrator privileges may be required to install software and updates, perform computer management tasks, or run certain software packages. Tasks should be performed using the most appropriate privilege level.

1.2 Reason for the policy
⇒ This standard will define how users are granted administrator privileges and the processes for requesting, granting/denying, appealing and revoking these privileges at Fisher College of Business.

1.3 Primary guidance to which this policy responds
⇒ This policy responds to the university “Local Administrator Privilege Standard”:

http://buckeyesecure.osu.edu/Policy/LAPS/

1.4 Responsible college office and officer
⇒ The Fisher College of Business Information Security Manager (ISM) is responsible for the maintenance of this standard and for responding to questions regarding this standard. The Fisher College of Business Chief Information Officer (CIO) is the responsible officer.

1.5 Who is governed by this policy
⇒ This standard applies to all individuals who access, use or control Fisher College of Business computer resources. The individuals covered include, but are not limited to faculty, staff, students, contractors, consultants, those working on behalf of the college, and/or individuals authorized by affiliated institutions and organizations.

1.6 Responsibilities
⇒ Users granted administrator privileges share the responsibility for the security of their system. Computer systems should be properly maintained and adhere to information security best practices. ITS and end users will work together to maintain a secure client environment.

⇒ Users granted administrator privileges have the ability to run and install software. Users must adhere to the End User License Agreement (EULA) associated with all software.

⇒ Administrative accounts are prime targets for viruses, worms, BOTS and other malicious infections. If administrative accounts are compromised, these infections can utilize this access to perform one of many malicious actions that could include taking control of the computer for malicious intent, spreading the infection to other machines in the college, or provide unauthorized access to restricted data. If a system is compromised, ITS will immediately prohibit the computer connection and retrieve the system to perform corrective actions.
Section 2. Policy Text

2.1 Introduction

⇒ Faculty and staff often have a legitimate need for administrator privileges on their computers. Administrator privileges are required to install software and updates, perform computer management tasks, or run certain software packages.

2.2 Default computer groups

⇒ All computers owned by Fisher College of Business will be classified into a default computer group. The default computer group will be based on the user(s) of the computer.

<table>
<thead>
<tr>
<th>Computer Group</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Faculty</td>
<td>A computer/device that is assigned and operated by a FCOB faculty member.</td>
</tr>
<tr>
<td>Lecturer</td>
<td>A computer/device that is assigned and operated by a FCOB lecturer.</td>
</tr>
<tr>
<td>Staff</td>
<td>A computer/device that is operated by a FCOB staff member.</td>
</tr>
<tr>
<td>Student Staff</td>
<td>A computer/devices that is assigned and operated by a student staff user.</td>
</tr>
<tr>
<td>PhD</td>
<td>A computer that is assigned and operated by a PhD candidate.</td>
</tr>
<tr>
<td>ITS</td>
<td>Computer and/or computer resources that are assigned or operated by ITS staff members.</td>
</tr>
<tr>
<td>Student Computer Lab</td>
<td>Computers that are utilized in a FCOB student computer lab.¹</td>
</tr>
<tr>
<td>Teaching/Research</td>
<td>Computers that are utilized in a FCOB teaching/research computer lab² or laptops utilized from the mobile laptop teaching carts.</td>
</tr>
<tr>
<td>Classroom</td>
<td>Computer that is utilized in a FCOB controlled classroom or on a mobile cart that is utilized in any FCOB space.</td>
</tr>
</tbody>
</table>

¹ FCOB student computer labs: Gerlach Hall 208 (graduate student only) Mason Hall 005 and 010 (undergraduate student only) Mason Hall 120

² FCOB teaching/research computer labs: Mason Hall 321 and 345
2.3 Default administrator privileges

⇒ Full administrator privileges: Administrator privileges are granted to a computer/device by default for all users.

⇒ Full administrator privileges with accountability statement: Administrator privileges are granted to a computer/device for all authorized users. Users must adhere to the Administrator Privileges Accountability Statement and review administrator privileges training guide.

⇒ No administrator privileges: Administrator privileges will not be granted to a computer/device.

<table>
<thead>
<tr>
<th></th>
<th>Full Administrator Privileges</th>
<th>Full Administrator Privileges with Accountability Statement</th>
<th>No Administrator Privileges</th>
</tr>
</thead>
<tbody>
<tr>
<td>Faculty</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lecturer</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Staff</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Student Staff</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PhD</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ITS</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Student Computer Lab</td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Teaching/Research Computer Lab</td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Classroom</td>
<td>X</td>
<td></td>
<td>3 FCOB users are granted full administrator privileges. Non-FCOB users have limited user privileges.</td>
</tr>
</tbody>
</table>
2.4 Request process

⇒ Users will be granted administrator privileges to their computer based on their defined computer group (section 2.2). Users will be provided the *Administrator Privileges Accountability Statement* and *Administrator Privileges Training Guide*.

⇒ Users who do not fit the established roles which allow administrator privileges may request an exception by contacting the ITS helpdesk. The Information Security Manager will respond to the request within 5 business days of receipt.

2.5 Appeal process

⇒ Users whose request for administrator privileges is denied or revoked may appeal the decision with the Office of Information Technology Services. The Information Security Manager will review the request with the CIO. The Information Security Manager will respond to appeal requests in writing to the requester within 10 business days.

⇒ Users who wish to appeal the decision of the Office of Information Technology Services may opt to involve the Fisher College of Business Senior Associate Dean and/or the University Chief Information Officer (or representative) for a final decision.

2.6 Approval duration

⇒ Due to the evolving nature of technology and the changing roles of users at the university, all default administrator privilege groups will be reviewed on an annual basis by the Information Security Manager.

2.7 Education requirements

⇒ Users who are granted local administrator privileges should complete the following steps:

- Review the *Administrator Privileges Training Guide*.
- Review the *Administrator Privileges Accountability Statement*. 
2.8 Privilege revocation

⇒ User administrator privileges may be revoked for the following reasons:

- User no longer serves in a role that requires administrator privileges.
- User abuses or demonstrates continued unsafe practices while using administrator privileges.
- System displays signs of compromise or risk of compromise.

⇒ Decisions to revoke user administrator privileges will be made collaboratively by Information Technology Services and the department chair or unit head based on documentation of any of the above conditions. Revocation of administrator privileges will be communicated in writing to the user upon execution.

⇒ Users may request reinstatement of their previously granted administrator privileges using the exception/appeal process. The decision process may consider the documentation and decision that led to the revocation in the restoration decision.
Section 3. Policy Reference

3.1 Contacts

⇒ Office of Information Technology Services, Fisher College of Business, The Ohio State University
   Web:  http://fisher.osu.edu/technology
   Email: helpdesk@fisher.osu.edu
   Telephone: 614-292-8976

3.2 Cross reference to related policies

⇒ For FCOB policies, see the Fisher College of Business Information Technology Services site:
   http://fisher.osu.edu/technology

⇒ For OSU security policies, see the Ohio State University Office of the CIO IT policies and the Buckeye Secure site:
   http://cio.osu.edu/policies/
   http://buckeyesecure.osu.edu/Policy/Index
Section 4. Glossary

4.1 Definitions

Administrator Privileges: Elevated privileges on a computer to complete configuration and software installation

BOTS: Software applications that run automated tasks over the Internet. Bots can be a malicious use in the coordination and operation of an automated attack on networked computers

CIO: Chief Information Officer

EULA (End User License Agreement): Software license agreement is a contract between the "licensor" and purchaser of the right to use computer software

FCOB: Fisher College of Business

IS: Information security

IT: Information technology

ISM: Information Security Manager

ITS: Information Technology Services

LAPS: Local Administrator Privilege Standard

OSU: The Ohio State University

Restricted Data: Data protected or regulated by law or critical to university operations (e.g., credit card information, SSN with name)

Security Controls: Safeguards or countermeasures to avoid, counteract or minimize security risks

System: A computer, storage, peripherals and associated software

Virus: A computer program that can copy itself and infect a computer

Worm: A self-replicating computer program that uses a network to send copies of itself to other computers
Section 5. Revision History

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
</table>
