Information Technology Services	**Document Type:** Policy
	Local Administrator Password Solution

Summary

This standard is a security standard that defines the use of Microsoft's Local Administrator Password Solution (LAPS) for use at the University of Kentucky and enterprise systems run by Information Technology Services (ITS). LAPS provides management of local account passwords of domain-joined computers. Passwords are stored in Active Directory (AD) and protected by Access Control List (ACL), so only eligible people can read it or request its reset.

Audience & Applicability

Anybody with local administrative rights on an Enterprise systems machine that is connected to the University of Kentucky AD domain. LAPS is available upon request for any department that is connected to the AD domain.

Intent

All enterprise systems will use LAPS for local account administration and password management. Any UK college or department can implement and use LAPS by following this Policy.

Full Policy

LAPS will be used on all UK Enterprise systems. Upon request, it is available to be used by all IT support administrators that work at the University of Kentucky. These requests can be made through ITS Customer Services: phone 859-218-HELP (4357) or email 218help@uky.edu.

To ensure password and system integrity only authorized users will be allowed to "reset/request" a local account password. These authorized users will be the listed beforehand as the account/machine administrator(s). The administrator should be listed in the "notes" section in AD when LAPS is added to the machine. The Department Business Officer must initiate request for an employee to be added to the Authorized Users list. LAPS accounts and administrators will be audited twice per year by the LAPS Administrator, who will purge inactive accounts.

Persons able to use or grant password resets are ITS domain administrators, enterprise administrators, qualified ITS service desk staff, and qualified ITS enterprise system administrators.

The process for vetting an administrator for rights to use LAPS for password resets rights will be to submit a request to the Cybersecurity, Data Privacy, and Policy.

All LAPS passwords should be considered administrator-level passwords and should adhere to the Standard For Elevated Rights Accounts.

Justification

In environments where customers are required to log onto computers without domain credentials, password management is a complex issue. The breadth of these environments greatly increase the risk of a Pass-the-Hash (PtH) credential replay attack. LAPS can help to eliminate the use of a common local account being tied to an identical password on every computer within a given domain. One way that LAPS does this is by setting a different, random password for the common local administrator account on each computer within the domain. Domain administrators using the LAPS solution can determine which user accounts, such as Helpdesk administrators, are authorized to read passwords.

LAPS simplifies password management while helping customers implement recommended defenses against cyber attacks. In particular, the solution mitigates the risk of lateral escalation that results when customers use the same administrative local account and password combination on their computers. LAPS stores the password for each computer's local administrator account in Active Directory, secured in a confidential attribute in the computer's corresponding Active Directory object. The computer is allowed to update its own password data in Active Directory, and domain administrators can grant "read access" to authorized users or groups, such as workstation Helpdesk administrators.

Exceptions

Exceptions to these standards are anticipated; all exceptions need to be requested and approved before they are implemented.

Exception requests should be submitted to ITS Customer Services at 859-218-4357 or 218help@uky.edu. Customer Services will then assign and forward the requests to the Cybersecurity, Data Privacy, and Policy Team for disposition. The Cybersecurity, Data Privacy, and Policy team dispositions can be appealed to the UK CIO.

Definitions

Elevated User Account. Any user who has the ability to change data or manipulate settings on enterprise systems that could impact the confidentiality, availability or integrity of the enterprise system.

Enterprise Systems. Enterprise systems are any UK hardware, software, virtual machine, database, application, router, switch, firewall, bridge, modem, wireless access point, and/or any item in UKs /ITS inventory that has the ability to impact other user's data, availability, integrity or confidentiality.

General User Account. Any UK active directory account that is emailed enabled. Meaning, the account has an email box enabled in active directory settings. So that a user can send and receive email l to that user's email account. This account can have only rights to non-elevated access and privileges, and must not be used to access enterprise systems.

ITS employee. Any employee that works for UK Information Technology Services.

Local Accounts

Administrator Account: The Administrator account is disabled by default, but you can enable it. When it is enabled, the Administrator account has full control of the computer, and it can assign user rights and access control permissions to customers as necessary. This account must be used only for tasks that require administrative credentials. It is highly recommended that you set up this account to use a strong password. For additional security considerations for accounts with administrative credentials. The Administrator account is a member of the Administrators group on the computer. The Administrator account can never be deleted or removed from the Administrators group, but it can be renamed or disabled. Because the Administrator account is known to exist on many versions of Windows, renaming or disabling this account will make it more difficult for malicious users to try and gain access to it. For more information about how to rename or disable a user account.

Guest Account: The Guest account is used by people who do not have an actual account on the computer. A customer whose account is disabled, but not deleted, can also use the Guest account. The Guest account does not require a password. The Guest account is disabled by default, but you can enable it.
You can set rights and permissions for the Guest account just like any user account. By default, the Guest account is a member of the default Guests group, which allows a user to log on to a computer. Additional rights, as well as any permissions, must be granted

to the Guests group by a member of the Administrators group. The Guest account is disabled by default, and it is recommended that it stay disabled.

Systems Account. A distinct UK active directory account that is NON-email enabled and used by UK employees to administer UK enterprise applications or hardware. This account will have the naming nomenclature of "SYSlinkblue" or "linkblue_SAD" Example: SYSDoe, DoeSAD. This account is to be used only to administer UK enterprise systems. Older or legacy SYS accounts can keep the original naming convention.

UK Employee. An individual who receives a paycheck and W-2 form from the University of Kentucky.

Document Change Log (This document is reviewed every 6 months for relevancy.)			
ITS Division Responsible	Cybersecurity, Data Privacy, and Policy		
Created On	November 15, 2017		
Approved On	April 12, 2018		
Approved By	Brian Nichols		
Date Revised/Reviewed	Prepared By	Role	Revision/Comments