DOUGLAS COUNTY ADMINISTRATIVE POLICIES AND PROCEDURES

NUMBER:	400.05
EFFECTIVE DATE:	8/29/2016
LAST REVIEWED:	05/19/2022
LAST REVISED:	05/19/2022
AUTHORITY	BOCC
COUNTY MANAGER	
PAGE	1 of 4

SUBJECT: PATCH MANAGEMENT POLICY

I. PURPOSE:

Douglas County's Technology Services Department (TSD) is responsible for ensuring the confidentiality, integrity, and availability of its data and that of customer data stored on its systems. TSD has an obligation to provide appropriate protection against malware threats, such as viruses, Trojans, and worms which could adversely affect the security of the system or its data entrusted on the system.

The purpose of this policy is to ensure computer systems attached to the Douglas County network are updated accurately and timely with security protection mechanisms (patches) for known vulnerabilities and exploits. These mechanisms are intended to reduce or eliminate the vulnerabilities and exploits with limited impact to the business.

Effective implementation of this policy will limit the exposure and effect of common malware threats to the systems within the scope.

II. SCOPE

This policy applies to all employees of Douglas County; as well as vendors, contractors, partners and any other parties, who use, work on, or provide services involving Douglas County computers, technology systems, networks, and/or data and will be subject to the provisions of this policy.

III. GENERAL POLICY:

All networked devices belonging to or managed by the TSD will be patched with vendor provided operating system security patches.

Users of desktop computers shall log-off their computers nightly to ensure critical patches can be applied to their machines.

Regular patching schedules will be implemented, and patches will be applied as soon as possible following appropriate testing of the security patches by the TSD staff.

New devices must be patched to the current patch level, as defined by the operating system vendor, PRIOR to the device being connected to the production network.

Current patch status for all Douglas County or other affiliated and partner organizations must be communicated to the Douglas County's Chief Technology Officer (CTO) or designate.

Devices that cannot be patched will be reported to the CTO or designate and the exact mitigation efforts will be documented and deployed.

A. Unsupported Software

Software no longer supported by the vendor will not to be installed on Douglas County production hardware. This includes operating systems and service packs or updates for these operating systems. While a vendor may support a certain operating system or software package, they may only specifically support that operating system of software at certain service pack or patch levels. In general, vendors also provide support retirement dates well in advance.

B. Service Packs

When a vendor releases a new major update/service pack for their software, including operating systems and office suite applications, TSD will deploy the service pack within three months of the release date. The three-month window provides time during which the software upgrade can be fully tested and subsequently deployed before support for the previous service pack level ends. This may also include entirely new versions of software, if deemed critical by the TSD Network Security Administrator (i.e., a new version of antivirus software).

C. Security Patches

Microsoft typically releases security patches on the second Tuesday of every month. The TSD Network Security Administrator (NSA) maintains the list of security patches and in some cases, the security patch may not carry the same severity rating that Microsoft has assigned. In most cases, the TSD-NSA will send notification informing TSD staff of upcoming patches, and their corresponding severity levels.

If there is an active outbreak of a virus or other critical issue to address that uses an exploit patched in a security patch, testing may be foregone, and the TSD Network Security Administrator may direct the TSD staff to immediately deploy the patch to all systems. In addition, any affected departments may be disconnected from the network until the outbreak is resolved.

D. Mobile Devices

Mobile devices such as laptops and Microsoft based tablets will have Global Protect installed and will connect to the network at least once a month to receive updates. Users will leave the device connected for at least 24 hours to ensure updates have sufficient opportunity to be applied. It is critical that users consistently perform this action prior to requiring the device to conduct Douglas County business so service is not disrupted as updates are applied.

Devices such as cell phones and tablets based on either Apple's iOS or Google's Android platform are the user's responsibility to maintain in a patched and up-to-date status. TSD will restrict access to Douglas County resources from devices that are out of compliance which may result in a user's loss of services such as email and calendar.

E. Monitoring and Enforcement

The TSD is to utilize automated solutions and other reporting mechanisms to monitor the enterprise computing resources and ensure that current software, service pack, and patch levels defined in the above policy are in place.

IV. EXCEPTIONS

A. Systems or applications that cannot be patched to resolve a known vulnerability will have the justification documented by the device/application owner, and necessary security controls will be implemented to mitigate the vulnerability until the system can be patched. The same is required in instances where patches are unable to be applied in a timely manner.

i. Justification

1. No patches from application vendor are available.
2. Patches create instability within the system, and the instability outweighs the risk.
3. Other reasons as approved by TSD Managers.

ii. Security Controls

1. Network segmentation
2. Access Control Lists
3. Host-Based Intrusion Prevention System

B. Systems that transmit or store protected data and cannot be patched to resolve a known vulnerability will be brought to the attention of the data owner. This information will be given to the Enterprise Security Team and necessary security controls to compensate for the vulnerability will be implemented.

V. DEFINITIONS

Term	**Definition**
Device	Any object used to store, process, and/or transfer data.
Enterprise Security Team	TSD Network Security Administrator, Senior Systems Engineer, and the Senior Computer Network Technician

Operating System (OS) Set of programs used to provide the basic functions of a computer.

Networked Device Any device that is either permanently or periodically attached to the Douglas County network.

Patch A piece of software designed to fix problems with or update a computer program or its supporting data

Trojan A class of computer threats (malware) that appears to perform a desirable function but in fact performs undisclosed malicious functions

Unsupported Software Software no longer supported by the vendor that produced it.

Virus A computer program that can copy itself and infect a computer without the permission or knowledge of the owner.

Worm A self-replicating computer program that uses a network to send copies of itself to other nodes. May cause harm by consuming bandwidth.

VI. RESPONSIBILITY FOR REVIEW:

The Internal Review Committee shall review this policy at least once every 3 years.