



District of Columbia Government – Office of the Chief Technology Officer

Patch Management Policy

Policy Number:	OCTO – 5010.1	Creation Date:	19 June 2017
CIS Top 20:	1, 2, 3, 4, 5, 6, 10, 13, 14, 17, 18, 19	Approval Date:	19 June 2017
NIST Control Family:	AM, RM, DS, IP, MA, PT, CM, RP	Revised Date:	N/A

1. Applicability. This policy applies to:

- 1.1. Executive Branch agencies, organizations, and personnel that fall under the direct authority of the Mayor of the District of Columbia.
- 1.2. Any agency or organization (City Council, Independent Agencies, D.C. Charter Schools, D.C. Courts, and others) that receive enterprise services from the Office of the Chief Technology Officer (OCTO) that this policy governs, but does not fall under the direct authority of the Mayor of the District of Columbia. This does *not* include non-profit organizations and other approved customers who subscribe to the D.C. Community Access Network (DC-CAN) services.

2. Authority.

- 2.1. DC Official Code § 1-1402 et seq., provides OCTO with the authority to provide information technology (IT) services, write and enforce IT policies, and secure the network and IT systems for the District government.

3. Operational Agreements

- 3.1. Memorandum of Understanding (MOU): DC organizations of any type, must enter into an MOU with OCTO as the baseline agreement for the IT services that they subscribe to, which sets forth the roles and responsibilities of each party to the MOU, and the process in which services will be billed to the agency and paid to OCTO.
- 3.2. Service Level Agreement (SLA): OCTO includes an SLA in the MOU for each OCTO service. The SLA defines the level of service expected from the service provider. SLAs are output-based in that their purpose is specifically to define what the customer will receive. They contain components such as reliability goals (e.g., “up-time”), responsiveness, procedures for reporting issues, level of monitoring (e.g., 24/7), and consequences of not meeting the SLA’s stated objectives. They may contain tiers for critical users, systems, and/or applications.
- 3.3. Interconnection Security Agreement (ISA): An organization must enter into an ISA with OCTO in order to connect its internal network or application to OCTO’s infrastructure.

The ISA is a security document that specifies the technical and security requirements for establishing, operating, and maintaining the interconnection. It also supports the MOU between the organizations.

4. **Overview.** The District government is responsible for ensuring the confidentiality, integrity, and availability of its data and constituent data stored on its systems. The District government has a legal obligation to mitigate system vulnerabilities and provide appropriate protection against malware threats, such as viruses, Trojans, and worms which could adversely affect the security of the system or data entrusted on its' systems. Effective implementation of this policy will remediate system vulnerabilities that are identified on a daily basis, and limit the exposure and effect of malware threats to the systems within this scope.
5. **Purpose.** The purpose of this policy is to establish a Patch Management program, as a subset of a larger Vulnerability Management Program, with patch management standards and processes that supports the requirements to inventory, apply, and track the patch status of all network resources to minimize risk to known vulnerabilities and inform decision-makers on the status of vulnerability risk to their systems, data, and mission.
6. **Scope.** This policy applies to:
 - 6.1. District assets – All servers, workstations, laptops, tablets, smartphones, network equipment, Internet of Things (IoT) devices, and any other computerized devices used to conduct official District government business or interact with internal networks and business systems, whether owned or leased by the District Government, the employee, or a third party.
 - 6.2. District workforce - Employees, contractors, consultants, temporary staff, interns, volunteers, and other personnel performing official information technology (IT) system administration and management functions at, or on behalf of the District Government, and general users of government IT.
 - 6.3. External parties – District business partners, vendors, suppliers, outsource service providers, and other third-party entities that utilize non-District government computers to access internal District networks and systems, or process official District government information, must ensure those specific computers are protected with the most current and properly applied patches.
7. **Policy.**
 - 7.1. **Servers.**
 - 7.1.1. All District government servers must be patched on a planned routine basis, and no greater than thirty (30) days for critical security patches or ninety (90) days for all other patches after the latest vendor patch release. Although three months provides a window of potentially significant risk even for medium and lower vulnerabilities, it is acknowledged that some applications require more extensive testing and troubleshooting prior to applying patches.
 - 7.1.2. All District government servers located in OCTO datacenters and/or connected to the internal enterprise network must utilize OCTO's enterprise patch management

solution to receive and apply patches. This allows for a central enterprise view of District patch status and risk, in which agency-specific dashboards and reports can be generated to inform agency leadership of risks to their mission.

7.1.3. At the time of this policy development, the District enterprise solutions for server patch management include, but not limited to:

7.1.3.1. HEAT for Microsoft Windows-based servers.

7.1.3.2. Satellite for Red Hat Enterprise Linux (RHEL) servers.

7.1.3.3. OPatch for Oracle-based servers and software.

7.2. Desktops and Laptops.

7.2.1. All District government desktops and laptops (also known as “endpoints”) must be patched on a planned routine basis, and no greater than thirty (30) days after the latest vendor patch release.

7.2.2. The District enterprise solution for endpoint patch management is LanDesk (Windows) and Casper (MAC). Per the District’s *Network Access Control policy*, every endpoint connected to the District government network must have the enterprise endpoint management application LanDesk installed and be managed by OCTO Helps.

7.3. Mobile Devices (Tablets, Smartphones, etc.).

7.3.1. All District government mobile devices (tablets and smartphones) must be patched on a planned routine basis, and not greater than thirty (30) days after the latest vendor operating system or application (“app”) patch release. This includes devices utilizing Apple iOS, Google Android OS, Blackberry OS, Windows Phone OS, or other mobile operating systems.

7.3.2. OCTO is coordinating with cellular telephone service providers and device manufacturers to implement an enterprise solution to update and manage District government mobile devices. This solution consists of:

7.3.2.1. District government iPhones will be added the Apple Device Enrollment Program (DEP) to remotely manage policies and update the iOS and installed apps.

7.3.2.2. District government Samsung Android telephones will be managed by Knox for policies and OS/app updates.

7.3.2.3. Until the two District enterprise patching solutions specified above are fully implemented, it is incumbent upon each user to apply mobile OS and app updates as they are made available by their respective vendors.

7.4. Network Devices (routers, switches, security appliances, etc.).

7.4.1. All District government network devices must be patched on a planned routine basis, and no greater than ninety (90) days after the latest vendor patch release. Due to the critical nature of core network infrastructure, and risk of disrupting enterprise network services with an untested patch, an attempt to balance this risk with the vulnerability risk will be made by allowing up to ninety (90) days to test, troubleshoot, and implement a solution to successfully apply patches.

7.5. **Common Vendor Patch Release Schedules.** Most operating system vendors have pre-planned patch release dates that will be used for the foundation of the District's routine patch schedule. However, there are some instances where a critical patch is released out of cycle due to the significant risk of the vulnerability. In those cases, District systems affected by the vulnerability must test and implement the out-of-cycle critical patch as soon as possible, but no greater than thirty (30) days after the vendor patch is released.

7.5.1. Microsoft. Microsoft releases new patches on the second Tuesday of each month in what is termed "Patch Tuesday". While it is highly recommended for all newly released patches to be applied within the first thirty (30) days, and required for critical patches, server owners may delay up to ninety (90) days to fully test how medium and lower patches will affect their system/application. All applicable patches within a release for a given OS version must be applied no later than 90 days after patch release. For example, server owners must apply the Microsoft critical patches released on January 15th no later than February 14th, and medium and lower patches no later than April 14th.

7.5.2. Oracle. Oracle releases new patches on a quarterly basis, around the 17th of the given month (January, April, July, and October). Due to the sensitivity and criticality of these servers and services, applicable patches are given more time for testing but must be applied prior to the next patch release (<90 days).

7.5.3. Red Hat. Red Hat releases new patches as they are developed, without any specific periodicity. Critical security patches must be applied within thirty (30) days and all other patches within ninety (90) days from the date of release. It is recommended that a monthly patch cycle is scheduled to apply all outstanding patches released in the previous 30-60 days.

7.5.4. Cisco. Cisco releases patches twice a year, in March and September. Applicable patches must be tested and applied within ninety (90) days.

7.5.5. Other Vendors. For those systems provided by vendors not listed above, the same standards for operating systems apply – critical patches must be applied within thirty (30) days, and medium and lower patches not greater than ninety (90) days.

7.6. **Monthly Maintenance Window.** OCTO has established a monthly maintenance window for all applicable systems to be patched by system owners. Those systems that do not have any patches to be applied may remain up and operational during maintenance window, or the system owner may use that time for other maintenance of the system as needed. It should be generally accepted that many services and systems may not be available during this period and that patches should be downloaded and staged prior to the maintenance window. If an agency or system owner requires the

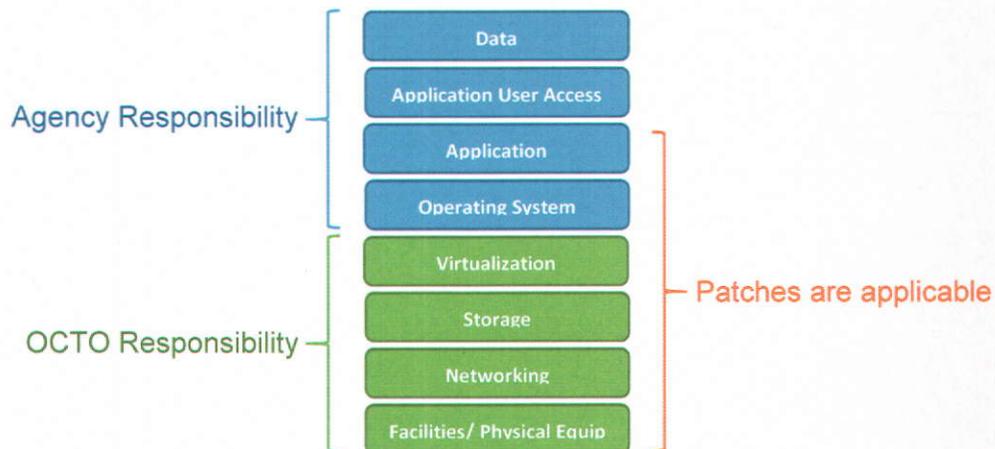
services of another system that they don't manage during the maintenance window, they need to coordinate with the other system owner at least one week prior to the maintenance window. The maintenance windows are as follows:

- 7.6.1. Development & Test (Dev/Test) Environment – From 8:00am on the first (1st) Thursday of each month to 4:00am the following Friday morning so that the patching can be done during or after normal working hours to allow the greatest flexibility. System owners will confirm successful application of patches and ensure that the system is working properly before applying the same patches to the production environment.
 - 7.6.2. Live Production Environment – First Friday of each month, 8:00pm to 4:00am after normal working hours. *(Note: This is only sixteen (16) hours after the Dev/Test) environment maintenance window ends).*
 - 7.6.3. Critical Out-of-Cycle Patching or Emergency Ad-Hoc Maintenance – OCTO and agencies will need to coordinate through the CCB process for any critical out-of-cycle patches or emergency ad-hoc required maintenance.
- 7.7. **End of Life “Legacy” and Unsupported Operating Systems and Applications.** Operating systems and applications that are end of life and no longer supported by their vendor pose significant risk to the network and District. By default, vendors do not develop or publish patches for unsupported operating systems and applications even when new vulnerabilities are discovered. Therefore, unsupported operating systems and applications are prohibited on the enterprise network. System owners must plan and coordinate with vendors and OCTO to ensure that operating systems and applications are updated prior to reaching end of life. All vendors publish a schedule specifying the end of life for their operating system and application versions and that no further support will be provided. It is incumbent upon the agencies and system owners to be aware of these dates and plan for such upgrades.
- 7.8. **Firmware Updates.** Those devices that utilize firmware (wireless access points, server/computer hardware, etc.) must be included in the patch management program. Firmware updates must be tested and applied within ninety (90) days of the latest patch release.
- 7.9. **The “Cloud”.** This policy also applies to virtual machines (VM) hosted in third-party service provider Infrastructure-as-a-Service (IaaS) cloud services, whether they are hosted in OCTO's virtual datacenter with Microsoft Azure or another cloud service provider.
- 7.10. **Applications.** Commercial off-the-shelf (COTS) and government off-the-shelf (GOTS) applications must be patched within thirty (30) days of the vendor releasing a new patch, and custom-developed applications must be updated prior to 180 days from the time an underlying framework or standard becomes end of life (e.g., .Net Framework, secure protocol, etc.). OCTO will patch managed servers and endpoints; however, it is incumbent upon agencies and system owners to coordinate with custom application development vendors well in advance to update their applications before an outdated component becomes a risk to the District.

7.11. **Change Management.** As an important component of a mature information technology service management program, managing changes to systems is critical to inform stakeholders, provide an opportunity for business and technical subject matter experts to weigh-in on potential impacts and timing, track changes and how they affect the system, and what may need to be undone if a change causes a negative impact to the system. Therefore, OCTO programs will utilize the Change and Configuration Board (CCB) process and Remedy ticketing system. Agencies will be required to use OCTO's CCB and Remedy ticketing system if and when they require change support from OCTO. It is also recommended that agencies managing their own systems and who do not require support from OCTO develop and use their own change management process, or leverage OCTO's existing CCB process and Remedy.

7.12. **"Beta" Programs.** Some vendors provide "Beta" testing programs that allow customers to download, install, and use software and updates that are not fully tested or made available to the general public/customer base as a means to gain feedback and resolve issues that can only be found outside of a lab environment. The use of "Beta" operating systems and software updates are not authorized for production use on any government IT system (network, computer, mobile, etc.). Only designated and OCTO-approved IT staff may participate in "Beta" testing programs on development / testing systems.

8. **Roles and Responsibility.** The District employs a shared responsibility model for managing the numerous IT systems and infrastructure. It is critical that all involved understand their role within this shared model depicted below.



8.1. **OCTO.** OCTO is responsible for drafting, implementing, and enforcing District information technology (IT) policies in support of federal and local laws, D.C. Municipal Regulations, Mayor's Orders, and District priorities to ensure appropriate guidance is provided to the DC Government workforce to minimize risk.

8.1.1. **Chief Technology Officer (CTO).** The CTO is ultimately responsible for the operation and protection of District enterprise information technology and data. The CTO will review waiver requests submitted by other Agency Directors, as outlined in paragraph 12 below, and approve or deny the request based on the overall risk to the District.

- 8.1.2. **Chief Information Security Officer (CISO).** The CISO establishes the patching requirements for system owners, monitors status, and enforces compliance. The CISO and his/her team will process and follow-up on waiver requests submitted by other agencies or OCTO program managers.
- 8.1.3. **Enterprise Cloud and Infrastructure Services (ECIS).** ECIS operates the patch management solutions for District government servers. They ensure newly published patches are immediately downloaded and made available to the District, notify agencies and system owners, test and apply patches to enterprise servers (e.g., Domain Controllers, Domain Name Service (DNS) servers, etc.), and monitor and provide a monthly report on District-wide server patch status. ECIS will provide written standard operating procedures (SOP) for how to install and use the enterprise patching software.
- 8.1.4. **OCTO Helps.** OCTO Helps operates the patch management solution for District government endpoints (desktops and laptops). They ensure newly published patches are immediately downloaded and made available to the District, coordinate with agencies and system owners, test and apply patches to enterprise endpoints and baseline images, and monitor and report on District-wide endpoint patch status.
- 8.1.5. **DC-Net.** DC-Net will manage patching for enterprise network and IoT devices, and manage the CCB process.
- 8.1.6. **OCTO Application Program Managers.** OCTO Program Managers (PMs) who manage enterprise applications and services will download newly published patches for the operating systems and applications under their responsibility, coordinate with agencies and customers, test and apply applicable patches, and monitor and report on their patch status.
- 8.1.7. **Governance, Risk, and Compliance (GRC) Division.** GRC is charged with drafting policy, advising OCTO and agencies on policy, and monitoring compliance to ensure more responsive and transparent IT Governance.

8.2. Agencies.

- 8.2.1. **Agency Director.** The Agency Director is the owner of the agency's risk profile. The Director is responsible to the Mayor, City Council, and District constituents to adequately protect against, and respond to risks to the agency's mission, personnel, facilities, data, and information systems. The agency Director may implement supplemental and supporting policies to this OCTO policy to address any agency unique needs and/or if the agency would like to be more restrictive. However, agencies may not publish policy that directly conflicts with OCTO policy. If the agency is unable to comply with a District IT policy or standard, the Director must submit a waiver request to the Chief Technology Officer for approval in accordance with paragraph 12 below. This request requires the Agency Director to accept the risk to their mission and data from being non-compliant, and provide a remediation plan with a timeline to become compliant.

8.2.2. **Agency Chief Information Officer (CIO) or Agency IT Manager.** The Agency CIO or IT Manager oversees and/or executes the District patch management program for their specific agency; coordinating with OCTO leadership and PMS regarding concerns, challenges, planning, and patching timelines.

8.2.3. **Agency Information Security Officer (AISO).** The ASIO is responsible for monitoring and enforcing the District's patch management policy for their agency; coordinating with system owners, the CISO, GRC Division, and OCTO technical leads.

8.2.4. **Agency System Owners (ASO).** Agency System Owners are responsible for the function, operation, management, and protection of their specific system(s). Specifically, in support of this policy, ASOs must coordinate with ECIS to implement the enterprise server patch management solution based on:

8.2.4.1. Agencies with no IT staff - ECIS will automatically apply all applicable patches in accordance with the schedule maintenance window discussed in paragraph 7.6 above. The ASO must monitor the status of patching for their systems, coordinate issues with ECIS, and report the status to their agency Director.

8.2.4.2. Agencies with an IT staff - The ASO or designated IT staff must manually test and apply patches provided by OCTO to each server, endpoint, network device, and application that comprises their "system" using the District enterprise patching solutions and within the timelines set forth in this policy. They must also provide a monthly patch status report to their agency CIO and OCTO highlighting overall percentage of compliance, overdue patches / issues, and if his or her agency is not compliant, provide a detailed plan for becoming compliant.

8.3. District Workforce.

8.3.1. Until the District enterprise patch management solution for mobile devices is in place, each member of the District Workforce who have been issued mobile devices (e.g., tablet or smartphone), are responsible for updating their assigned mobile device operating system (e.g., Android or iOS) and installing applications within thirty (30) days after an update is released. Typically, mobile device operating systems and apps provide a visual cue that an update is available. In addition, a monthly check of updates from the device's App Store will show available updates that need to be installed.

9. **Procedures.** Upon the effective date of this policy, agency CIOs/IT Managers must review the requirements and their role in monitoring and enforcing the policy. OCTO PMS will update and publish standard operating procedures (SOP) for their services to the District (e.g., patch software, CCB process, etc.) on the District Intranet at <https://octo.in.dc.gov> under "Policy & Governance". All District personnel, employees and contractors, must read and abide by the policy.

10. **Policy Maintenance.** OCTO is responsible for the maintenance, administration, and publication of this policy. OCTO will annually review this policy and update as needed to ensure the policy's technical relevance and regulatory compliance.
11. **Policy Enforcement.** All Mayoral agencies and personnel, and all non-Mayoral customers of the services in which this policy applies, are responsible for abiding by, enforcing, and reporting all identified non-compliance matters. OCTO is ultimately responsible to the Mayor, City Council, and constituents for monitoring and enforcing this policy through implementation and oversight of security controls, coordination with agency CIOs, and internal assessments. Agencies must actively participate in the audit of this policy when requested by OCTO.
12. **Exemptions, Exceptions, and Waivers.** Waiver requests for specific patches must be submitted by the Agency Director to OCTO's GRC division at compliance.octo.dl@dc.gov for processing and to obtain CTO approval. The request is a standard OCTO letter format that states that the Agency Director is accepting all risk to their agency mission and data, provides the details why compliance cannot be met, and sets forth a plan and timeline indicating when the agency can achieve compliance by applying the patch(es) in question. The letter template can be found at <https://octo.in.dc.gov/service/octo-policies>.
 - 12.1. **Non-Executive Branch Organizations and Independent Agencies.** Those organizations that do not fall under the authority of the Mayor may choose to opt-out of the District enterprise patch management policy and solutions. However, specific network security controls will be placed between the enterprise and those organizations so that any risk accepted by them for not patching their systems will not result in increased risk to the District as a whole. These security measures could potentially impact some enterprise services subscribed to by the independent organization. However, some of these enhanced security measures may not be necessary if those organizations that choose to opt-out provide monthly status reports of their server and endpoint patching progress to demonstrate self-compliance.
13. **Sanctions.** If OCTO discovers that an agency or organization is not in compliance with this policy, OCTO will:
 - 13.1. Advise the agency CIO of the non-compliance and assist them, if necessary, in developing a corrective action plan and a reasonable timeframe for its implementation.
 - 13.2. If the agency CIO does not implement the corrective action plan within the stated timeframe, OCTO will escalate the matter to the agency Director for immediate action and resolution.
 - 13.3. If the agency Director does not resolve the policy non-compliance within his/her agency, OCTO will refer the matter to the City Administrator for immediate action and resolution.
 - 13.4. OCTO may disconnect network connectivity and/or suspend affected services to the non-compliant agency for organizational non-compliance, and depending on the severity and risk to the District.
 - 13.5. OCTO may suspend an individual user's network and application accounts, and their agency Director and/or DCHR may take personnel disciplinary actions for an individual's non-compliance depending on the severity and risk to the District.

14. References.

- 14.1. DC Official Code § 1-1402, *et seq.*
- 14.2. National Institute of Standards and Technology (NIST) Cyber Security Framework (CSF)
- 14.3. NIST Risk Management Framework (RMF)
- 14.4. NIST Special Publication (SP) 800-40 r3 – Guide to Enterprise Patch Management Technologies

15. Effective Date(s). This policy shall be effective upon the date the CTO signs the document, and will remain in effect until superseded or cancelled in writing.

16. Revision History.

Date of Change	Responsible Entity	Summary of Changes
19 June 2017	OCTO / CWITS / GRC Div.	Complete rewrite

17. Policy Acceptance.



Archana Vemulapalli
Chief Technology Officer
Government of the District of Columbia

6/26/17
Date