-->

DNS Standard

Last Modified on 06/26/2026 2:18 pm EDT

For more details about the Information Security Office, **please visit our website**!

1. Purpose and Scope

The purpose of this document is to establish a Domain Name System (DNS) Standard at Wharton. It aims to protect school resources, ensure appropriate delegation, and maintain compliance with applicable regulations. This standard prevents conflicts in namespaces under the University umbrella. Additionally, it designates where alternate namespaces may be appropriate to maintain a trusted ecosystem adherent to School and University Policies and Standards. This standard is informed by University Policies particularly: the University's IT Network Policy, Wharton's Information Security Policy, the University Accessibility Standards, and Wharton Marketing and Communication's brand Identity Guidelines.

The DNS Standard applies to all students, faculty, staff, contractors, vendors, and any individuals or entities managing Domain Name System resources within Wharton owned or managed domains.

This document presumes that any implementation requiring DNS components has been through a Security Risk Review Assessment as defined by the Security and Privacy Risk Review Standard. Any deviation from this standard not addressed with the Risk Review Standard process will require adherence to the Wharton Exception Policy.

2. Definitions

The following definitions will cover foundational concepts, local terminology or define general terms to the scope of this document.

- **DNS:** Domain Name System
- **DNS Domain:** A specific name with DNS, it's associated records. It may be a top-level domain (TLD) like .edu, second level domain like http://upenn.edu or third level (+) domain like wharton.upenn.edu
- **DNS Namespace:** A hierarchical segment of DNS names. For this document the wharton.upenn.edu namespace refers to the third level domain as well as any fourth level or above domains within it.
- **DNS Subdomain:** A label prepended to a domain that creates a separate segment to manage. The wharton.upenn.edu domain is a subdomain of http://upenn.edu .
- **DNS Third Level Domain:** A subdomain prefix directly adjacent to a second level domain. According to University IT Network Policy Wharton is assigned the wharton.upenn.edu Third Level Domain. Wharton is responsible for a selection of additional third level domains in the http://upenn.edu namespace as approved by the University.
- **DNS Zone:** A managed segment of the DNS namespace. Where a subdomain is a logical segment of a namespace, a Zone is an administrative segment defining management boundaries. Every zone begins at a subdomain boundary. Not every subdomain boundary creates a zone.

- **Domain Control Validation:** The use of a DNS record by a third party to verify the ownership of a domain.
- **Limited-Scope Email Service**: A service, often a bulk mailing platform, intended for limited forms of email communication (su. Generally subject to its own technical controls and process oversight.
- **General-Purpose Email Service:** A service that accepts interpersonal business communication associated with a user or users for the University.
- **Network Names and Numbers (NNN):** The University System of Record for DNS configurations. https://nnn.upenn.edu
- **PennNet:** The range of IP addresses managed by the University. https://itpm.azurewebsites.net/Elements/ShowDocument?path=060&doctitle=IT%20Network%20Policy

3. Standards

All approvals in this standard are facilitated by the Wharton Information Security Office's Risk Review Standard unless otherwise noted. ISO will navigate various authorized parties on the requestor's behalf relevant to the namespace in question.

3.1 University Namespace

The Wharton School's governance of University namespace falls into three primary categories: the principal third-level domain at wharton.upenn.edu; additional third level domains authorized by the University for Wharton's use; subdomains of the third-level domains.

Before a record in the Wharton Managed Namespace is directed at a resource external to PennNet that resource must first be approved.

DNS Records no longer in association with active resources must be released in NNN as soon as possible, at most within two business days of decommissioning. Inactive records make it difficult to present an accurate inventory and, in some cases, present inherent security concerns.

3.1.1 Wharton Managed Namespace DNS Record Requirements

3.1.1.4 MX Record

MX (Mail Exchanger) Records identify the mail servers responsible for accepting email for a domain.

Any General-Purpose Email Service must make use of the University mail hygiene platform or another approved solution.

3.1.1.9 TXT Record

TXT (Text) Records stores arbitrary text, often used for email security (SPF, DKIM) or domain verification. Specific types of TXT records are detailed below.

TXT Records may also be used for Domain Control Validation see section 3.1.2

3.1.1.9.1 SPF Record

SPF (Sender Policy Framework) Records designate authorized email servers for the associated domain. All SPF records in Wharton Managed Namespaces require approval. A SPF record allows sending from any address within

the domain and this review ensures, in part, that adequate controls are in place. SPF Records for external services should target DNS records over IP addresses wherever possible.

3.1.1.9.2 DMARC TXT Record

All Wharton Managed Namespaces must default to the use the University record at _dmarc.upenn.edu unless otherwise approved.

3.1.1.10 CAA Record

CAA (Certificate Authority Authorization) Records restricts which Certificate Authorities can issue SSL/TLS certificates for a domain. An unapproved certificate provider may become restricted by a CAA record.

Creation and management of a CAA record within the Wharton Managed Namespace requires approval.

3.1.2 Domain Control Validation

CNAMES or TXT records may be used by third parties to confirm ownership of the University namespaces before allowing certain configurations. These configurations can grant broad authority and can potentially preclude multiple configurations. No Domain Control Validation (DCV) records shall be configured for services that have not been approved.

Wharton Computing shall maintain a record of: all configured DCV records; their requestor and team; the service they are offered for; if the service re-verifies and the re-verification window; the intended functionality and the scope of authorization.

See section 3.1.4.1 for specifics about Domain Control Validation records in the wharton.upenn.edu namespace.

3.1.3 Namespace Delegation

Delegation of Wharton Managed Namespaces may be considered to meet operational needs. Any service delegated access to a portion of the wharton.upenn.edu namespace is still obligated to adhere to this standard and must be approved. DNSSEC (DS Record) is required along with any Name Server (NS Record) delegation. Any delegation of Wharton Managed Namespace must maintain support for IPv6.

Wharton Computing shall maintain a record of: all configured namespace delegations; their requestor and team; the service they are offered for; and what services are being used in the delegated namespace.

Control of Wharton Managed Namespace via NS Records may not be delegated outside of University owned or managed systems.

3.1.4 Primary Third Level Domain

The Wharton School's primary third level domain within the University system is wharton.upenn.edu. The School's namespace is under the direct administration of Wharton Computing.

3.1.4.1 Domain Control Validation

Any service requiring Domain Control Validation (DCV) in the Primary Third-Level Domain must either be managed directly by Wharton Computing or not preclude additional implementations of the service. An existing DCV record that is found to conflict with a service to be run for the school, the pre-existing service must accept reconfiguration or discontinuation in coordination with Wharton Computing.

3.1.4.1.1 Domain Claiming

Domain Claiming is usually associated with Domain Control Validation and is used to describe a variety of mechanisms that allow for a third-party tool to claim broad control of resources linked to a namespace. Examples include associating all email addresses with a given domain with a given product instance or requiring all management of domain and subdomain entries on the platform from one account. Domain Claiming on services associated with wharton.upenn.edu may only be done and administered by Wharton Computing.

3.1.4.1.2 DKIM

DKIM (DomainKeys Identified Mail) is a specific form of DCV that authorizes a third party to cryptographically sign messages on behalf of the institution. This prevents tampering with message content and is a control against phishing. These records may be managed by CNAME or TXT record. DKIM values should be rotated at least annual and should be unique to each account from the third party or have understood mitigated control established through a risk review.

3.1.3.2 A Records

A Records associate a domain name to an IPv4 address or addresses. Any A Record for the wharton.upenn.edu namespace must be configured through the University Network Names and Numbers (NNN) Service or through services delegated through NNN. A Records must be determined to be appropriate and sufficiently unambiguous.

The appropriateness of an A Record is a combination of reasonable evaluation by subject matter experts for concerns and assessing the authority of the requesting party and vetted with relevant stakeholders when a value might be contentious.

The ambiguousness of an A Record is established by the record having a clear meaning and being unlikely to conflict with other requests. Acronyms, if they have multiple meanings that might cause confusion, should be avoided. If multiple stakeholders, such as an administrative department and an academic department might have overlapping interests, those should be assessed collectively prior to approval.

3.1.3.3 AAAA Records

AAAA Records map a domain name to an IPv6 address or addresses. AAAA Records should be created and applied to all systems with an A Record. All requirements appropriate to A Records also apply to AAAA Records unless otherwise noted.

3.1.3.4 CNAME

A CNAME (Canonical Name) creates an alias, pointing one domain or subdomain to another. CNAMEs are exclusive of other record types (MX, TXT, etc.) for the same name. A CNAME, like an A Record, must be determined to be appropriate and sufficiently unambiguous.

CNAME Flattening which returns the destination IP rather than returning the appropriately aliased DNS value is not supported within the NNN service.

A CNAME may also be used for Domain Control Validation see section 3.1.3.1

3.1.4 Additional Third-Level Domains

Additional Third-Level Domains are not as directly tied to the Wharton brand and may have different governance bodies than the wharton.upenn.edu primary third level domain. Additional Third-Level Domains will be subject to the same review and controls as wharton.upenn.edu unless alternate documented authorization and/or standards have been submitted to Wharton Computing and approved by Wharton Computing operational staff and stakeholders.

3.1.5 Subdomains

Fourth Level and beyond domains allow for more flexible delegation and looser governance and restrictions. Specifically, subdomains do not have the obligation to safeguard the ability to host centralized services for the school. When considering naming of resources at the Fourth Level or beyond more flexibility is available as the subdomains lead to less likelihood of ambiguity. Sponsors of a subdomain are assumed to be subject to the requirements of this standard absent an approved alternate standard.

3.1.5.1 Domain Control Validation

Domain Control Validation (DCV) may be requested at the Fourth Level domains or beyond. So long as these DCV records don't preclude or impact configurations at parent domains without approval they can be configured as appropriate according to the requirements of approved services and the owner of the subdomain.

3.2 Non-University Namespaces

Some University offerings will be hosted outside of the Penn Namespace, either by intent or as a requirement of an external platform. Wherever possible Wharton services and resources should be hosted within a Wharton Managed Namespace.

3.2.1 Partner Services

Not all external services can be run within a Wharton Managed Namespace. These usually operate within the partner namespace, sometimes within a Wharton subdomain. It is neither possible to ensure all partner services can offer a Wharton subdomain, nor that a Wharton subdomain is operated by appropriate Wharton resource. If a partner service can operate with the Wharton Managed Namespace that configuration must be pursued. If a partner cannot operate within a Wharton Managed Namespace these services should be accessed initially from within Wharton Managed Namespaces as a means of acknowledging the partnership.

3.2.2 Unaffiliated Namespaces

Unaffiliated Namespaces refer to domains outside the http://upenn.edu domain that Wharton or Centers associated with Wharton own and operate. These are generally managed by third party domain registrars such as http://register.com or cloud platform providers like Amazon Web Services. External Namespaces may not be used to offer production Wharton services without approval. Any offering in an unaffiliated domain is still obligated to adhere to University policy.

3.2.3 Lookalike Domains

Lookalike domains are domains that give a general appearance of being associated with the University yet reside outside of the http://upenn.edu or wharton.upenn.edu namespace. **You must not use lookalike domains for end-user-accessible production services.**

Lookalike domains are often used in phishing and scam campaigns and the use of them prevents user ability to distill legitimacy of content.

4. Compliance

ISO will compile and provide reporting on adherence to this Standard and related policy to key leaders and stakeholders in the institution including the COO/CFO, CIO, CISO and the Executive Director of Human Resources and People Operations.

Services running in Wharton Managed Namespaces not in compliance with Wharton Standards may have their records revoked.

Services that do not meet an acceptable level of compliance through a Risk Review Assessment will be required to receive a formal Exception. Absent a formal exception, DNS resources referencing services that do not adhere to Wharton's Standards may have their records revoked.