YesGov

GOVERNMENT DOMAIN SECURITY REPORT

hkdpl.org

Haverstraw King's Daughters Public Library District, New York

Checked October 21, 2026 at 8:53 PM UTC · Check ID b7da5b72-503d-4811-80f0-d6f62fda4dbb

D

5 of 16 checks passed **Residents are exposed**

Basic protections recommended by CISA are missing. Each fix below is a standard setting, listed in order of risk to residents.



5 passed 11 missing

Website	Email	DNS and domain
3 of 8	0 of 5	2 of 3

Not on a .gov domain

hkdpl.org is not a .gov address. Anyone can register a look-alike .com or .org, so residents cannot tell from the address alone that this is the official site.

CISA and DHS advise that .gov is a requirement for secure government, trusted communication and public trust. Every day on a non-.gov address is a day residents can be fooled by an impostor site or email.

What to fix first

In order of risk to residents. Each is a one-time setting that then needs to be watched.

1. **Add a DMARC policy** — HIGH RISK

   Nothing tells receiving servers to reject mail that falsely uses this domain, so fake bills and payment requests in the agency's name are delivered.

   Fixed by: Your email or DNS provider

2. **Publish an SPF record** — HIGH RISK

   Receiving mail systems cannot tell the agency's real email from a forgery, so residents can receive fake notices in its name.

   Fixed by: Your email or DNS provider

3. **Turn on DKIM signing** — HIGH RISK

   Outgoing mail is not signed, so receivers cannot confirm it came from the agency, and DMARC cannot be fully enforced.

   Fixed by: Your email provider

4 **Turn on DNSSEC** — HIGH RISK
DNS answers are not signed. A forged answer can send residents to a fake payment page, or redirect the agency's email, with no visible sign.
Fixed by: Your DNS host and domain registrar

5 **Turn on HSTS** — MEDIUM
On public Wi-Fi, a resident's visit can be pushed to an unencrypted copy of the site.
Fixed by: Your web host

6 **Require encrypted mail delivery (MTA-STS)** — MEDIUM
Mail sent to agency staff can be forced onto an unencrypted connection and read in transit.
Fixed by: Your email or DNS provider

7 **Turn on mail encryption reports (TLS-RPT)** — MEDIUM
Nobody is told when encrypted mail delivery to the agency fails or is tampered with.
Fixed by: Your DNS provider

8 **Add framing protection** — MEDIUM
The site can be hidden inside a hostile page to trick residents into clicking buttons they cannot see.
Fixed by: Your web host

9 **Add a CAA record** — MEDIUM
Any certificate authority in the world may issue a certificate for this domain, which makes impersonating the site easier.
Fixed by: Your DNS provider

10 **Add file type protection** — MEDIUM
Browsers may guess file types, which can let an uploaded file run as code against visitors.
Fixed by: Your web host

11 **Publish a security contact (security.txt)** — MEDIUM
People who find a security problem have no standard way to tell the agency before it is misused.
Fixed by: Your web host

All results in detail

Every record and value we saw, grouped by area. Written for your IT team, readable by anyone.

Website — 3 of 8 passed

HTTPS certificate — PASS

Issued by	**WE1**
Issued to	**hkdpl.org**
Expires	**December 11, 2026 (50 days after this check)**
TLS version	**TLSv1.3**

Redirect to HTTPS — PASS

HTTPS available	Yes
Plain address redirects to HTTPS	Yes

HSTS — MISSING

HSTS header	Not sent

What this means: On public Wi-Fi, a resident's visit can be pushed to an unencrypted copy of the site.
How to fix: Send the Strict-Transport-Security header with a max-age of at least one year. (Your web host)

Certificate trust and match — PASS

Trusted chain	Yes
Strong public key	Yes
Valid signature	Yes
Name matches domain	Yes

CAA record — MISSING

CAA record	Not found

What this means: Any certificate authority in the world may issue a certificate for this domain, which makes impersonating the site easier.
How to fix: Publish a CAA record naming the authority you use, for example 0 issue "letsencrypt.org". (Your DNS provider)

Framing protection — MISSING

X-Frame-Options	Not sent

What this means: The site can be hidden inside a hostile page to trick residents into clicking buttons they cannot see.
How to fix: Send the header X-Frame-Options: SAMEORIGIN, or a Content-Security-Policy with frame-ancestors 'self'. (Your web host)

File type protection — MISSING

X-Content-Type-Options	Not sent

What this means: Browsers may guess file types, which can let an uploaded file run as code against visitors.
How to fix: Send the header X-Content-Type-Options: nosniff. (Your web host)

Security contact (security.txt) — MISSING

/.well-known/security.txt	Not found

What this means: People who find a security problem have no standard way to tell the agency before it is misused.
How to fix: Publish /.well-known/security.txt with a contact address and an expiry date. (Your web host)

Email — 0 of 5 passed

SPF — MISSING

SPF record	Not found

What this means: Receiving mail systems cannot tell the agency's real email from a forgery, so residents can receive fake notices in its name.
How to fix: Publish one TXT record that lists every service sending mail for the domain and ends in -all. (Your email or DNS provider)

DKIM — MISSING

Signing keys	Not found

What this means: Outgoing mail is not signed, so receivers cannot confirm it came from the agency, and DMARC cannot be fully enforced.

How to fix: Turn on DKIM in the mail service (Microsoft 365, Google Workspace and others) and publish the DNS records it gives you. (Your email provider)

DMARC — MISSING

DMARC record	Not found

What this means: Nothing tells receiving servers to reject mail that falsely uses this domain, so fake bills and payment requests in the agency's name are delivered.

How to fix: Publish a TXT record at _dmarc with p=quarantine or p=reject and an address to receive reports. (Your email or DNS provider)

MTA-STS — MISSING

DNS record	Not found
Policy file	Not found
Enforced	No

What this means: Mail sent to agency staff can be forced onto an unencrypted connection and read in transit.

How to fix: Publish an _mta-sts TXT record and a policy file at mta-sts.(domain)/.well-known/mta-sts.txt. (Your email or DNS provider)

TLS-RPT — MISSING

TLS-RPT record	Not found

What this means: Nobody is told when encrypted mail delivery to the agency fails or is tampered with.

How to fix: Publish a TXT record at _smtp._tls with an address to receive reports. (Your DNS provider)

DNS and domain — 2 of 3 passed

DNSSEC — MISSING

Zone signed	No
Result	No DNSSEC records found. DNSSEC may not be enabled for this domain.

What this means: DNS answers are not signed. A forged answer can send residents to a fake payment page, or redirect the agency's email, with no visible sign.

How to fix: Turn on DNSSEC signing at the DNS host, then add the DS record at the registrar. (Your DNS host and domain registrar)

IPv6 — PASS

Website reachable over IPv6	Yes
Website IPv6 addresses	2606:4700:3035::6815:357, 2606:4700:3030::ac43:8283
Name servers reachable over IPv6	Yes

RPKI route protection

PASS

Website route signed	Yes
Website route valid	Yes
Name server route valid	Yes

.gov domain

NOT SCORED

Ends in .gov	No

What this means: Anyone can register a look-alike .com or .org, so residents have no way to confirm this is the official site. Every .gov request is verified by CISA.

Hosting and platform

Informational, not scored

Website server	**172.67.130.131**
Mail server	**None found**
Website server reputation	**Not on abuse lists**
WordPress	**Not detected**
Email addresses published on the site	**0**
Broken links found	**0**
Referrer policy header	**No**

Progress over time

Checks passed at each scan, oldest to newest. Highest possible is 16.



If these basics were missed, what else has been missed?

These are published CISA standards that any IT department or provider can check in seconds. YesGov can fix all 11 in under 24 hours, re-run this check to prove it, and keep watching every day. The move to .gov takes 1 to 2 weeks because CISA verifies each request; security fixes on the current domain do not wait for it.

yesgov.com/contact · (888) 777-0017 · info@yesgov.com

How we check

We only check settings that any computer on the internet can see: DNS records, certificates, web headers and mail policies. We never log in to, scan or probe any agency system. The 16 checks build on CISA Binding Operational Directive 18-01 and other published internet standards. Full method: yesgov.com/open-data#how-we-grade.

Verify this report online

Scan the code or visit the address below to see these results, check the domain again and get alerts when anything changes.

https://yesgov.com/check/hkdpl--org?check=b7da5b72-503d-4811-80f0-d6f62fda4dbb

YesGov PBC is a Public Benefit Corporation that works only with U.S. government agencies. 1639 Medical Center Parkway, Murfreesboro, TN 37129. This report reflects public settings at the time of the check and is not a full security audit.