

How DMS protects donor data

Your donors trust you with their name, address, phone number, PAN and giving history. This document sets out exactly how that information is protected, what each temple's data is separated from, and – just as importantly – what we do not claim.

DMS runs on Amazon Web Services in the Mumbai region, so all donor data stays in India. Every control described here is in place today and can be demonstrated on request.

YOUR DATA STAYS IN

India

Mumbai region. Donor records never leave the country.

BACKUPS

Cannot be deleted

Held in a locked vault. Not by us, not by an administrator, not by AWS support.

RECOVERY POINT

Under 5 minutes

The database can be restored to any moment, plus daily and monthly copies.

01 Your temple's data is separated from every other temple's

This is the first question every temple asks, so it is worth answering precisely. DMS is multi-tenant – several temples run on shared infrastructure – but each temple's data is held apart at every layer where it matters.

Donation records

Each temple has its **own separate database**, reached by its **own database user with its own password**. One temple's credentials cannot read another temple's records.

Receipts & documents	Each temple has its own private storage bucket . Permissions are written so a temple's application can reach only its own bucket.
Login sessions	Each temple has a unique cryptographic application key . A session or cookie issued by one temple's site is meaningless on another's — cross-temple impersonation is not possible.
Configuration	Each temple's settings and secrets are supplied to its application at run time and are never built into the shared software image , so one temple's credentials are never present in another's deployment.
Shared, and openly so	Temples share the underlying database server, the application image and — for smaller sites — a host machine. Separation is enforced by credentials and permissions, not by separate hardware. A dedicated server can be arranged where a temple requires it.

02 Donor records are encrypted and access is bounded

Encrypted at rest

The database, every server disk, every backup and every stored file is encrypted. Encryption is enforced by default, so a new disk cannot be created unencrypted by mistake.

Encrypted in transit

Every site is served over HTTPS with a valid certificate, and browser sessions are marked secure so they cannot travel over an unencrypted connection.

Receipts and identity documents are private

Donation receipts, Aadhaar images and donor documents are not publicly reachable. They are served only through the application, to a logged-in user, or through a signed link that expires. We test this boundary directly: public artwork returns 200, donor material returns 403.

The database is not reachable from the internet

It accepts connections only from the application servers.

Email is authenticated

Receipts are sent through Amazon SES from verified sending domains with DKIM signing, so receipts are far less likely to be spoofed or land in spam.

03 Donation records cannot be destroyed

Most systems can be restored from backup. The harder problem is a backup that someone — an intruder holding an administrator's password, or an administrator making a mistake — can delete before or after the damage. DMS is built specifically against that case.

Backups are held in a compliance-locked vault

Daily and monthly copies are written into a vault sealed in **compliance mode**. Once written, a copy cannot be deleted or shortened before its retention expires — **not by an administrator, not by the account's root user, and not by AWS support**. The lock itself is permanent and cannot be lifted.

This matters because deleting the backups is the standard second step of a serious attack. Here it is not available.

Point in time	The database can be restored to any moment within the retention window, typically to within about three minutes of now.
Daily	A full copy of the database every night, kept 30 days , in the locked vault.
Monthly	A month-end copy kept two years , for long-term records and 80G reporting.
Servers	Every server is imaged nightly and kept 14 days , so a lost machine is rebuilt rather than reconstructed. New servers are enrolled automatically.
Deletion protection	The database and every server carry deletion protection, so removing one is a deliberate two-step act, never a slip.

04 We can tell when something is wrong

Prevention is never complete, so detection is treated as a first-class control rather than an afterthought.

Continuous threat detection

Amazon GuardDuty watches API activity, DNS, network flows, storage access, database logins and server volumes for signs of compromise, using AWS threat intelligence.

A tamper-proof audit trail

Every administrative action across every region is logged, and the log store is **write-once**

— records cannot be deleted for a year, even by an administrator. Erasing the evidence is a normal part of a serious intrusion; here it is not possible.

Immediate alerts if a protection is switched off

Turning off logging, threat detection, a storage protection or a backup rule raises an alert within about a minute. Any use of the account's root login alerts as well.

Configuration recording and daily compliance checks

Every configuration change is recorded with a timeline, and the account is re-checked daily against the CIS Benchmark and AWS security best practice.

Network traffic records

Connections to and from the servers are recorded, so a security question can be investigated after the fact rather than guessed at.

05 **Access to the system is tightly held**

Two-factor, no exceptions	Every administrative login requires multi-factor authentication, including the account's root login. Passwords are a minimum of 14 characters with rotation and reuse limits.
No standing passwords in the software	The application servers hold no stored access keys . They authenticate using short-lived credentials issued automatically and rotated by AWS, so there is no long-lived secret to leak.
No public administrative access	Remote administration is not exposed to the internet at all. Only web traffic — ports 80 and 443 — is reachable from outside , in every region. Staff access is brokered through an authenticated AWS service.

	an authenticated AWS service.
Least privilege	Each application's permissions are scoped to its own storage and its own sending identity, and restricted to its own server's network address.
Dormant access is removed	Unused accounts and permissions are reviewed and deleted rather than left in place.

06 The service stays available, and repairs itself

Automatic recovery from failure

If a server's operating system hangs it is rebooted automatically; if the underlying hardware fails the server is moved to healthy hardware, keeping its address and its disks.

Applications restart themselves

Each temple's application is health-checked continuously. If it stops responding it is restarted automatically, without waiting for anyone to notice.

Early warning before exhaustion

Memory, database load and storage are monitored, and alerts fire while there is still time to act rather than after an outage.

Domains protected

All domains carry transfer locks and automatic renewal, and DNS is signed with DNSSEC so visitors cannot be silently redirected to a fraudulent copy of a donation page.

07 What we do not claim

A security document that lists only strengths is not much use in judging a supplier. These are the limits of what is in place today, stated plainly.

Please read this section as carefully as the others

- **We hold no formal certification.** DMS is not SOC 2, ISO 27001 or PCI-DSS certified, and has not been independently audited against those frameworks. The controls described here are real and demonstrable, but they are our own implementation, not a certified one.
- **Card and bank details are never held by DMS.** Payments are completed by the

- **Card and bank details are never held by DMS.** Payments are completed by the payment gateway. That is deliberate — it means a compromise of DMS cannot expose card data — but it also means payment security is the gateway's responsibility, not ours.
- **Temples share infrastructure.** Separation is enforced by credentials and permissions rather than separate hardware. This is normal for systems of this kind, and we would rather state it than imply otherwise.
- **There is no 24/7 staffed security desk.** Detection runs continuously and alerts are automatic, but response depends on a small team during working hours.
- **Administrators can still change the system.** Backups and audit logs are locked against deletion, but other protections can be altered by someone holding administrator access. Such a change raises an immediate alert; it is not blocked outright.
- **Recovery has a floor of a few minutes, not zero.** Point-in-time recovery trails live data slightly. In the worst case a restore may lose the last few minutes of donations, which would then be reconciled against the payment gateway's own records.

08 What we ask of you

Most donor-data incidents in systems of this kind begin with a person, not a server.

One login per person, never shared

Shared accounts make it impossible to tell who did what, and impossible to revoke access