

# Status & Incident Communication (Trust)

*Minimal status page spec with machine-readable feeds (RSS + JSON). Objective-only; not an SLA.*

**Document ID:** MVG-STATUS-1.0.2

**Version:** 1.0.2

**Effective date:** 2026-02-10

**Status:** Public

Formats: PDF (controlling) • DOCX (convenience)

**Classification:** Trust documentation (public-safe)

**Contact:** security@meridianverity.com (security) ? procurement@meridianverity.com (procurement)

## 1. Purpose

This document provides ready-to-publish copy and implementation guidance for MVG's public status page. Goal: reduce uncertainty for reviewers and buyers by publishing incident history and a clear communication posture.

Non-goal: create an uptime warranty, SLA, or contractual commitment for the public website.

## 2. Scope (what the status page covers)

- Public website availability (meridianverity.com) and public downloads/verification entry points.
- Optional: public-facing Proof Playground (/verify) availability.
- Enterprise Services (customer deployments) are governed by customer agreements; if a status is published for those, it must be explicitly scoped per product/tenant.

## 3. Status categories (recommended)

- Operational
- Degraded performance
- Partial outage
- Major outage
- Maintenance (scheduled)

## 4. Uptime objective (objective only)

Recommended copy:

“Uptime objective: We target high availability for the public site. This is an objective, not a warranty or SLA.”

If an outage affects procurement review (e.g., downloads or verification entry points), state an alternative delivery path:

“If something blocks your review, email us and we will provide an alternate delivery path.”

## 5. Machine-readable feeds (high signal for security & procurement)

Publish two machine-readable endpoints alongside the human-readable page:

- /trust/status (HTML) — human-readable status page.
- /trust/status.json (application/json) — canonical machine-readable status snapshot.
- /trust/status.rss (application/rss+xml) — incident update feed.

Design constraints (nitpick-proof):

- No user tracking. No subscription tracking pixels. RSS/JSON must not require cookies.
- No personal data in feeds. Keep incidents public-safe (do not publish sensitive exploit details).
- Set correct Content-Type and X-Content-Type-Options: nosniff.
- Use short caching for JSON/RSS (e.g., 60–300s) with ETag/Last-Modified; use longer caching for incident detail pages if versioned.
- Include a schema/version field in JSON so reviewers can pin parsers.

## 5.1 Suggested JSON shape (status.json)

Minimal fields (stable for automation):

- schema\_id (e.g., mvg.status@v1)
- site
- updated\_utc
- overall\_status
- components[] (id, name, status, notes optional)
- incidents[] (id, title, start\_utc, end\_utc optional, status, impact, updates[])
- subscribe (rss\_url, json\_url, human\_url)
- contacts (security, procurement)

## 5.2 RSS guidance (status.rss)

- Publish an item per incident update (or per incident) with a stable GUID.
- Do not include sensitive details; keep to impact + mitigation + resolution summary.
- Link each item to the human incident page (if you publish per-incident pages).

## 6. Incident communication fields (what to publish)

- Incident ID and start time (UTC) — plus detection time if known.
- Affected components (site, downloads, verify, etc.).
- User impact summary (plain language).
- Current status and mitigations/workarounds.
- Resolution time and brief root-cause summary (public-safe).
- Preventive actions (public-safe).

## 7. Support and alternatives (neighbor-first)

Recommended copy:

- “If something blocks your review, tell us. We will provide an alternative format or alternate delivery path.”
- “Security vulnerabilities are not handled through the status page. Report privately to security@meridianverity.com.”

## 8. Disclaimers (critical for legal durability)

- “This status page is informational and does not modify any contract.”
- “No SLA is provided for the public website unless expressly stated in a signed agreement.”
- “Incident details may be limited to protect security and ongoing investigations.”

## 9. Contact

- 
- Procurement routing: procurement@meridianverity.com
- 

## Change log

- v1.0.2 — Condensed layout; standardized PDF/DOCX roles; clarified non-SLA language.
- v1.0.1 — Added RSS + machine-readable JSON guidance; strengthened headers/caching guidance.
- v1.0.0 — Initial publication.