CONTINUITY HUB • WORKING PACK

Precautionary Outage Plan Pack: PHP Oct 21 Shutdown Checklists & Logs

OPERATIONAL WORKING PACK • $7 TIER
Current version — Nov 1, 2026. Update history: https://continuityhub.org/how-should-an-organization-plan-a-precautionary-outage-when-a-critical-vulnerability-cannot-be-patched-at-once/

SHEET 1: STANDING PHP INVENTORY & HIDDEN-COPY EXPOSURE REGISTER

CISA & COALITION STANDARD

Mandatory Pre-Emergency Requirement: CISA warns PHP prevalence is frequently unobservable as an embedded component. Coalition highlights administrative tools managing firewalls, databases, phone systems (PBX), and backups. PHP 8.1 and older receive zero project patches. Maintain this register with named owners and verified patch routes.

System / Asset Name	Exposure Tier	PHP Mode / Bundle	Version	EOL? (8.1-)	Named Owner	Defined Patch Route
Firewall Admin Portal Host: fw-admin.internal	Admin Tool (Internal)	Vendor Appliance (PHP-FPM)	8.1.18	YES (EOL)	NetOps Lead: _____	Vendor OEM Firmware Hotfix #412
Database Admin (phpMyAdmin) Host: pma.corp.lan	Admin Tool (VPN/Local)	Apache mod_php	8.2.14	NO	DBA Team: _____	Apt upstream repo → 8.2.35+
PBX / VoIP Phone Console Host: voice-pbx.telecom	Admin Tool (Internal)	FreePBX / php-cgi bundle	7.4.33	YES (EOL)	Telecom: _____	Isolate from LAN → Vendor Backport
Enterprise Backup Console Host: backup01.infra	Admin Tool (Restricted)	Vendor Appliance (PHP-FPM)	8.3.10	NO	Storage Admin: _____	Appliance Patch Bundle v12.4
Primary Customer Web Portal Host: www.company.com	Public Internet-Facing	PHP-FPM + Nginx pool	8.3.22	NO	Web Ops: _____	CI/CD Container Build → 8.3.36+
Hosting Control Panel Host: panel.sharedhosting	Internet & Admin Tool	cPanel / Plesk internal PHP	8.1.27	YES (EOL)	Hosting Ops: _____	cPanel Automated Tier-1 Update
Internal Intranet / Wiki Host: wiki.corp	Internal Staff Tool	FrankenPHP / Docker	8.4.15	NO	IT Support: _____	Docker image update → 8.4.27+
_____	[ ] Internet [ ] Admin [ ] Internal	[ ] FPM [ ] Apache [ ] Appliance	_____	[ ] YES [ ] NO	_____	_____
_____	[ ] Internet [ ] Admin [ ] Internal	[ ] FPM [ ] Apache [ ] Appliance	_____	[ ] YES [ ] NO	_____	_____
_____	[ ] Internet [ ] Admin [ ] Internal	[ ] FPM [ ] Apache [ ] Appliance	_____	[ ] YES [ ] NO	_____	_____
_____	[ ] Internet [ ] Admin [ ] Internal	[ ] FPM [ ] Apache [ ] Appliance	_____	[ ] YES [ ] NO	_____	_____

EOL PHP ISOLATION CERTIFICATION (PHP 8.1 & OLDER)

Coalition Rule

The PHP Project does *not* release security patches for PHP 8.1, 8.0, 7.x, or 5.x. For each EOL asset identified above, certify action:

- ☐ **Immediate Network Isolation:** Public internet routing disabled; restricted strictly to local subnet/management VLAN.
- ☐ **Vendor Backport Verification:** Formal vendor confirmation obtained that CVE-2026-109618/19 backports are compiled.
- ☐ **Precautionary Shutdown:** Service stopped pending platform migration.

Certified by Incident Commander: _____ *Date/Time:* _____

OPERATIONAL WORKING PACK • $7 TIER
Current version — Nov 1, 2026. Update history: https://continuityhub.org/how-should-an-organization-plan-a-precautionary-outage-when-a-critical-vulnerability-cannot-be-patched-at-once/

SHEET 2: IMPACT TOLERANCE & PRECAUTIONARY DECISION-RULE WORKSHEET

EVERBRIDGE FRAMEWORK

Calm-Condition Decision Framework: A precautionary outage balances vulnerability exposure against maximum tolerable disruption. Define the exact order of preference (Patch in-place → Isolate from internet → Take fully offline) and the actionable threshold for night-shift execution.

Important Business Service	Impact Tolerance (Max Disruption)	Deploy & Verify Window (Hours)	Preference Order & State Threshold	Execution Trigger Condition
Customer Order Processing Direct revenue channel	**4 Hours** Tier 1 Critical	Est: 1.5 hr patch + 1.5 hr test = **3.0 hr**	1. Patch in place 2. Maintenance mode queue 3. Full server stop	If staging patch fails QA at T+2h → route orders to offline queue and take PHP web servers offline.
Public Marketing Site Information only / lead gen	**24 Hours** Tier 3 Support	Est: 1.0 hr patch + 1.0 hr test = **2.0 hr**	1. Isolate to CDN static cache 2. Full offline	Freeze dynamic PHP origin immediately; serve static edge HTML; patch at standard maintenance window.
Client Billing & Invoicing Internal recurring batches	**12 Hours** Tier 2 Core	Est: 2.0 hr patch + 3.0 hr test = **5.0 hr**	1. Network isolate 2. Patch in place 3. Halt cron daemon	Disable incoming webhook port; if vendor patch unconfirmed by T+4h → stop PHP billing worker pool.
Customer Support Desk Ticketing & live chat	**6 Hours** Tier 1 Critical	Est: 2.0 hr patch + 2.0 hr test = **4.0 hr**	1. Failover to SaaS 2. Offline internal portal	Switch DNS to external fallback support portal; immediately power down on-prem PHP ticketing host.
_____	_____ Hours	_____ Hours	1. _____ 2. _____ 3. _____	_____
_____	_____ Hours	_____ Hours	1. _____ 2. _____ 3. _____	_____
_____	_____ Hours	_____ Hours	1. _____ 2. _____ 3. _____	_____

NIGHT-SHIFT ACTIONABLE THRESHOLD AUTHORIZATION

Executive Sign-Off

Pre-Approved Decision Rule (Mandatory CISA Default Enforcement):
"We will take the service offline if a fixed version cannot be deployed and verified within the window our impact tolerance allows. If a critical system cannot be updated at once, it goes offline until patched or isolated."

Authorized Incident Commander: .....
Title / Operational Role: .....
Signature:
Night-Shift Primary On-Call: .....
Emergency Contact (Phone/Signal): .....
Authorization Effective Date:

OPERATIONAL WORKING PACK • $7 TIER
Current version — Nov 1, 2026. Update history: https://continuityhub.org/how-should-an-organization-plan-a-precautionary-outage-when-a-critical-vulnerability-cannot-be-patched-at-once/

SHEET 3: OUTAGE SEQUENCING CHECKLIST & EXPIRING BRIDGE-MEASURE LOG

TECHNICAL REMEDIATION

SECTION A: OUTAGE & REMEDIATION SEQUENCING CHECKLIST

Execution Clock

Remediation order follows exposure risk: Administrative control tools first (Coalition), internet-facing systems first (CISA). Verify each step before moving down the stack:

☐	**Step 1: Admin Tools First**	Isolate or patch firewall, database, backup, and PBX web interfaces. Terminate active management sessions.	Time: _____ By: ____
☐	**Step 2: Internet-Facing Web**	Deploy official security releases to public web tiers. Fallback: take offline if deploy window > tolerance.	Time: _____ By: ____
☐	**Step 3: Target Version Audit**	Confirm binary version: **8.5.12**, **8.4.27**, **8.3.36**, or **8.2.35** or later (`php -v`).	Time: _____ By: ____
☐	**Step 4: Worker Pool Restart**	**MANDATORY:** Restart `php-fpm`, Apache (`httpd`), or worker service. Flush opcache and shared memory.	Time: _____ By: ____
☐	**Step 5: Distro Vendor Parity**	Where Linux distro or control panel packages are used, confirm vendor security advisory explicitly lists CVE fix.	Time: _____ By: ____
☐	**Step 6: Valtori Staged Testing**	Execute canary testing in staging before routing production traffic. (Valtori rule: verification > install).	Time: _____ By: ____

SECTION B: EXPIRING BRIDGE-MEASURE LOG (INTERIM HARDENING ONLY)

TEMPORARY STATE

PHP & CISA Explicit Caveat: Bridge settings reduce specific attack path exposure but **do not make an installation safe**. Every measure below represents a dated, expiring operational state with a hard deadline by which the service is either patched or taken completely offline.

Bridge Measure Configured	Applied Date/Time	Admin Name	Residual Risk & Attack Surface	Hard Patch-or-Offline Deadline
session.upload_progress.enabled = 0 Workers restarted in php.ini	2026-10-21 14:00	SysAdmin: _____	Blocks multipart session upload vector; non-multipart RCE vectors remain open.	**2026-10-22 02:00** (12h Max) **Action or Offline**
memory_limit locked Cannot be overridden by scripts	2026-10-21 14:15	SysAdmin: _____	Reduces OOM crash cascade; does not prevent remote payload execution.	**2026-10-22 04:00** [ ] Patched [ ] Offline
post_max_size minimized Restricted to 2MB or disabled	2026-10-21 14:20	SysAdmin: _____	Constrains payload size; small shell payloads remain functional.	**2026-10-22 04:00** [ ] Patched [ ] Offline
WAF Virtual Patching Rules Cloudflare/AWS WAF regex rules	2026-10-21 14:45	SecOps: _____	Inspects HTTP headers/body; protocol evasion and HTTPS bypass possible.	**2026-10-22 12:00** (24h Max) [ ] Patched [ ] Offline
_____	_____	_____	_____	_____

SHEET 4: PRE-APPROVED HOLDING STATEMENTS & COMPROMISE-CHECK SHEET

HUB & COALITION STANDARDS

SECTION A: PRE-APPROVED HOLDING STATEMENTS (HUB INTERNATIONAL STANDARD)

Communications

Draft holding statements *before* the outage. Precautionary framing highlights deliberate pro-security action:

Standard Holding Statement Template:
"As part of our commitment to system security, [Organization] has initiated a temporary precautionary maintenance outage affecting [Exact Services Taken Offline]. On October 21, 2026, the PHP Project issued emergency security bulletins (CVE-2026-109618 and CVE-2026-109619, CVSS 9.2). In accordance with federal cybersecurity directives, our technical team is deploying official updates and conducting comprehensive staging tests. No customer data compromise has occurred. The next operational status update will be issued at [Exact Time/Timezone]."

Audience	Channel & Distribution	Authorized Spokesperson	Comms Log & Timestamp
External Customers	Status page, portal banner, email blast	Customer Experience VP: ____	Sent: _____ [ ] Logged for Crestview
Internal Workforce	All-hands email, Slack announcement	CIO / HR Lead: _____	Sent: _____ [ ] Logged for Crestview
Key Vendors / Partners	Direct B2B liaison notification	Supply Chain Lead: _____	Sent: _____ [ ] Logged for Crestview
Executive / Board	Incident Commander flash report	CISO: _____	Sent: _____ [ ] Logged for Crestview

SECTION B: TIMESTAMPED COMPROMISE-CHECK SHEET (COALITION & CISA INDICATORS)

FORENSIC INTEGRITY

Separate Precautionary Defense From Unexplained Intrusion: Coalition saw active exploit requests >5 hours prior to patch. Documenting *"we looked, and here is what we found"* with exact timestamps protects insurance recovery and legal defense.

Forensic Indicator (CISA / Coalition)	Inspection Command / Method	Timestamp	Result Status	Analyst Initials & Evidence Log
1. Shells & CLI Downloads PHP spawning /bin/sh, curl, wget	`ps aux | grep -E '(sh|bash|curl|wget)'` Auditd / EDR process tree inspect	2026-10-21 __:__	[ ] Clean (Not Found) [ ] **COMPROMISE FOUND**	Analyst: _____ Log: audit_ps.log
2. Web Root Alterations New/modified files in document roots	`find /var/www -mtime -2 -ls` Git diff / Tripwire / FIM verify	2026-10-21 __:__	[ ] Clean (Not Found) [ ] **COMPROMISE FOUND**	Analyst: _____ Log: fim_scan.txt
3. Persistence & Account Changes New cron jobs, system user accounts	`crontab -l` across users; inspect `/etc/passwd`, shadow, sudoers	2026-10-21 __:__	[ ] Clean (Not Found) [ ] **COMPROMISE FOUND**	Analyst: _____ Log: cron_diff.log
4. Upload Bursts & OOM / 500s Upload requests + memory crash surges	Web server access log analysis: status 500 bursts + OOM syslog	2026-10-21 __:__	[ ] Clean (Not Found) [ ] **COMPROMISE FOUND**	Analyst: _____ Log: http_500.csv
5. Crashing PHP-FPM Workers Repeated segfaults / worker restarts	`dmesg | grep segfault` PHP-FPM master log termination checks	2026-10-21 __:__	[ ] Clean (Not Found) [ ] **COMPROMISE FOUND**	Analyst: _____ Log: dmesg_fpm.log

OPERATIONAL WORKING PACK • $7 TIER
Current version — Nov 1, 2026. Update history: https://continuityhub.org/how-should-an-organization-plan-a-precautionary-outage-when-a-critical-vulnerability-cannot-be-patched-at-once/

SHEET 5: INSURER-READY CLAIM DOCUMENTATION PACK & VALTORI RESTORATION PLANNER

BEAZLEY & CRESTVIEW AUDITS

BEAZLEY FORENSIC ACCOUNTING PACK — Financial Proof

Beazley published claims guidance establishes the exact records requested by forensic accountants to substantiate business interruption losses:

- ☐ **Daily Operational Records:** Transaction counts, processing volumes, and revenue receipts during outage window vs same days prior year.
- ☐ **Monthly Billings & Collections:** Minimum 12–24 months trailing collections history establishing baseline revenue velocity.
- ☐ **Prior Federal/State Tax Returns:** Form 1120 / 1065 verifying baseline profitability and overhead expenses.
- ☐ **Monthly Profit & Loss (P&L):** Financial statements for trailing 12 months signed by CFO/Controller.
- ☐ **Weekly Payroll Logs:** Overtime costs, standby pay, and standard payroll for loss window vs prior year.
- ☐ **Scheduling Logs:** Production run cancellations, service appointments deferred, and documented make-up hours completed.

CRESTVIEW TECHNICAL EVIDENCE PACK — Adjuster Standards

Crestview Public Adjusters technical documentation list for cyber business interruption claim settlement:

- ☐ **System Logs & Forensics:** Server event logs, syslog archives, and CISA/Coalition negative compromise diagnostic.
- ☐ **IT Downtime Duration Reports:** Uptime monitoring alerts (Pingdom/Datadog) verifying exact start, duration, and restore timestamps.
- ☐ **Customer Comms Logs:** Documented customer notifications, service disruption notices, and delivery impact logs.
- ☐ **Extra-Expense Invoices:** Vendor consulting bills, emergency patch engineering invoices, and cloud failover surcharges.
- ☐ **Broker/Carrier Notice Trigger:** Formal written notice to cyber broker/underwriter logged within policy notice period.

VALTORI RESTORATION TIMELINE PLANNER (DAYS-TO-WEEKS STAGED RESTORATION) — Reuters Report

Finland's state IT provider Valtori demonstrated that precautionary outages require days or weeks because restoration entails thorough verification alongside software updates. Plan staged restoration gates:

Restoration Phase	Technical Gate Criteria	Estimated Duration	Sign-Off Authority	Completion Time
Phase 1: Isolated Sandbox	Deploy 8.5.12/8.4.27/8.3.36/8.2.35+; run full automated regression test suite	6 – 12 Hours	QA Lead: _____	Passed: _____
Phase 2: Canary Web Node	Route 5% internal staff traffic; monitor worker crashes, OOM, and 500 errors	12 – 24 Hours	SecOps Lead: _____	Passed: _____
Phase 3: Public Traffic Cutover	DNS and load balancer cutover; WAF active; 24h continuous log monitoring	24 – 48 Hours	Incident Commander: ___	Passed: _____
Phase 4: Full Return to Service	All background workers active; make-up batch runs initiated; claim pack archived	Days to Weeks	CISO / Executive: ____	Certified: _____

BROKER & CARRIER NOTICE TRIGGER SHEET — Notice Compliance

Policy Carrier: ..... Policy Number: ..... Waiting Period (Hours): .....

Broker Contact: ..... Notice Given Date/Time: ..... Claim Reference Number: .....