Guardian Compliance for Nonprofits and Associations

How PTS Guardian tiers deliver the donor data stewardship, grant security attestations, and board-ready evidence your mission depends on.

The business problem: A nonprofit's most valuable asset is donor trust, and that trust now travels with personally identifiable data: giving history, ACH and credit card details, member rosters, and sometimes health or political affiliation. IRS Form 990 asks directly about your governance and data practices. State charitable solicitation registrations renew annually. PCI DSS applies the moment a donor enters a card number. Federal grants and an increasing number of foundation grants flow security requirements down through grant agreements. Most small and mid-sized nonprofits have the intent but not the documented program to prove it to a board, an auditor, a grantor, or a state attorney general.

The PTS answer: Guardian Compliance is our tier purpose-built for mission-driven organizations with fiduciary data obligations. It combines our managed help desk, cybersecurity, backup, M365 E5 cloud, and vCIO management with the Written Information Security Program, audit-ready evidence, and board-ready summaries your donors, members, grantors, and board audit committee expect. **Compliance is the tier that documents the stewardship your mission already promises.**

THE SOLUTION

Why the Compliance tier

Compliance is the Guardian tier built end-to-end for organizations where donor and member trust is the operating capital. Six capabilities make the difference between mission intent and documented stewardship:

- **M365 E5 with Purview, DLP, and Message Encryption.** Donor-record data loss prevention, audit log retention, and encrypted external email. The control set foundation grantors and cyber insurance underwriters now require.
- **Written Information Security Program (WISP) and IR Plan.** Documented policies covering donor privacy, payment data, member confidentiality, and breach response. Maps to your IRS Form 990 governance disclosures and state breach notification duties.
- **Air-gapped monthly server backups, performed and tested by PTS.** Demonstrable contingency for ransomware. The single most effective control against the wave that hit Blackbaud customers, the ICRC, and Planned Parenthood LA.
- **Phishing-resistant MFA on every remote access path.** Email, VPN, RDP, admin, and SaaS via SSO. The most-exploited gap in nonprofit BEC wire fraud cases like Save the Children, and the first item on every grantor security questionnaire.
- **Sub-processor and vendor inventory with risk reviews.** CRM, fundraising platform, payment processor, event registration, member portal, and email tool all touch donor and member data. PTS maintains the inventory, contractual safeguards, and annual review log.
- **Annual training, phishing simulation, and tabletop exercise.** Staff, board, and volunteer awareness. Documented completion records retained for grantor audits, board reviews, and state charitable solicitation renewals.

WHAT YOU GET

Inside the Compliance tier

A single managed-service bundle that delivers the help desk, security, backup, M365 E5 cloud, and vCIO management your organization's fiduciary obligations depend on. Each layer is included in the monthly fee.

Service Layer	What you get
Help Desk	Remote, on-site, and emergency support within monthly limits. Acknowledge under 1 business hour, on-site under 8 business hours. 25% discount on after-hours emergency. Coverage scales to event and campaign launches.
Cybersecurity	Advanced endpoint detection and response, 24/7 managed detection and response, phishing simulations and training, application allow-listing, DNS filtering, full-disk endpoint encryption, SIEM with compliance logging, network monitoring.
Backup	Image-based cloud backup (workstations and servers), 3x 2TB external drives included, monthly air-gapped server backups performed by PTS, monthly restore testing logged for board, grantor, and audit committee evidence.
Cloud (M365 E5)	M365 E5 nonprofit licensing where eligible, Purview audit logs, DLP for donor and member data, Message Encryption, email and file backup, DDoS protection, DNS and domain management.
vCIO / IT Leadership	Quarterly TBR, PTS firewall and network standards, vendor and sub-processor management, 100+ policy templates including WISP, Donor Privacy, Acceptable Use, IR Plan, and breach notification scaffold. Annual written report for the board and audit committee.

Why one bundle, not piecemeal tools

Most nonprofits and associations accumulate a patchwork: a fundraising CRM, a separate email tool, an accidental IT person on staff, a donation processor someone set up years ago, and a privacy policy copied from a peer org. Guardian Compliance replaces that stack with one accountable provider whose evidence binder maps directly to your IRS Form 990 disclosures, state registrations, PCI obligations, and grantor security attestations.

What it takes	Piecemeal	Phantom Bundle
Vendor count	6 to 10 separate contracts: MSP, SOC, EDR, backup, M365, training	One contract, one invoice, one accountable provider
Documentation	ED assembles WISP and privacy policies from each tool	PTS maintains WISP, IR Plan, donor privacy and breach scaffold
Restore testing	Backup vendor sells software; ED self-tests or skips	Monthly air-gapped restore performed and logged by PTS
Grantor questionnaire response	ED scrambles to answer each foundation and federal grant survey	One call to PTS, attestations and evidence delivered from binder
Sub-processor accountability	Each fundraising and member SaaS tracked independently	PTS maintains sub-processor inventory and annual risk reviews
Single point of escalation	Incident response routes through each vendor's separate support	P1-P4 escalation through one MSP, board-ready timeline on day one

One contract. One WISP. One accountable provider. That is the difference between mission intent and the documented stewardship your donors, members, and grantors expect.

THE PROOF

The cost of getting it wrong

Nonprofits and associations are a soft target: rich donor data, lean IT, frequent volunteer turnover, and high reputational exposure. The figures below are public-record settlements, ransom payouts, and BEC losses. Small orgs are not exempt, they just rarely make headlines.

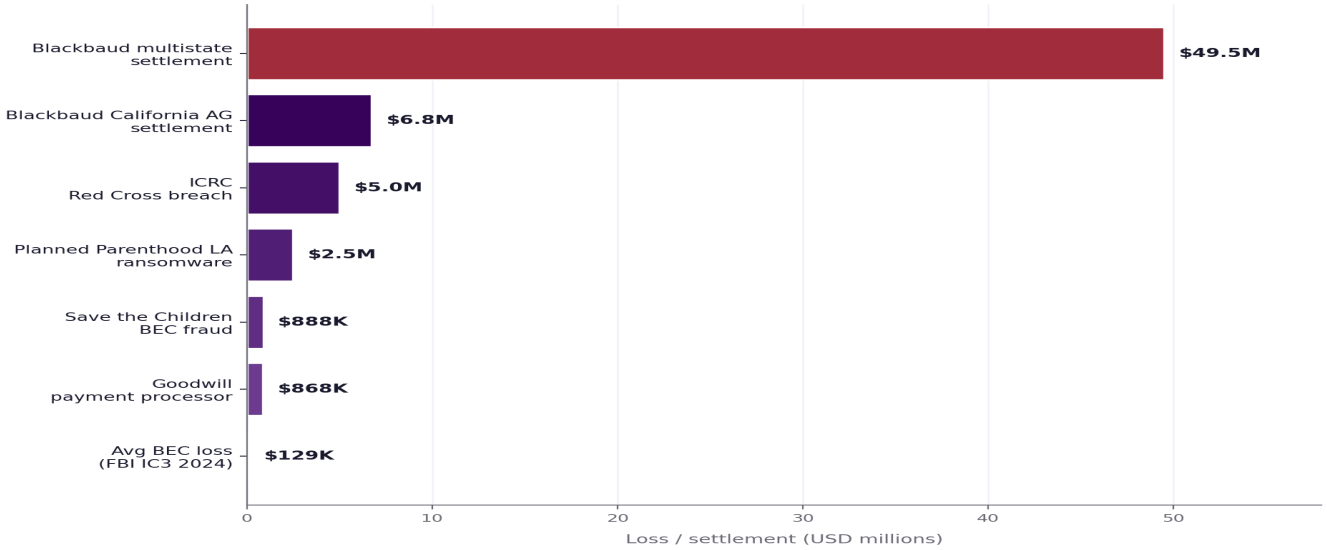
$49.5M
Blackbaud multistate settlement covering 13,000+ nonprofits and universities

515K
Individuals exposed in the 2022 ICRC Red Cross breach

$129K
Average BEC loss per incident in the FBI IC3 2024 report

Form 990
IRS governance section that asks about your data and policy practices

Public-record nonprofit cyber impact.



Settlement amounts, ransom payouts, and BEC losses from state attorney general filings, FBI IC3 reports, and organization statements. Beyond the dollar figure, each org above also faced donor and member departure, board crisis management, grantor questions, and reputational impact that the disclosed number does not capture.

Three patterns we keep finding in nonprofits

PATTERN 01

MFA on email, not on the donor database

VPN, RDP, fundraising CRM, and finance system still password-only. The most-exploited gap in nonprofit BEC wire-fraud cases including Save the Children's $1M loss. Phishing-resistant MFA on every entry point closes it.

PATTERN 02

Sub-processor sprawl across the donor record

Fundraising CRM, peer-to-peer platform, payment processor, event registration, email tool, and donor research service all touch the donor record. Most orgs have no inventory, no risk reviews, and no contract language. Grantors now ask for this list.

PATTERN 03

No WISP, no IR Plan, no board-ready scaffold

State breach notification laws apply to donor and member PII. Most orgs have no WISP, no decision tree, and no board communication template. The result is a frozen response when the audit committee chair calls.

THE DETAIL

Mapped to nonprofit obligations and CIS Controls

Page 4 pairs each nonprofit obligation with the Guardian capability that delivers it. Page 5 shows the CIS Controls v8.1 baseline that implements those obligations in practice. Skim the Compliance column, every YES is documented and audit-ready.

IRS FORM 990 - Governance and disclosure of data practices

Citation	Requirement	How Guardian Delivers	Co-Mgd	Fund.	Compl.
Form 990 Pt VI	Governance section: disclose written policies for conflicts of interest, whistleblower, document retention, and joint ventures. Auditors increasingly extend this to data and privacy policies.	Documented WISP, donor privacy policy, document retention schedule, board-approved policy library. Annual written report aligns with audit committee review.	NO	YES	YES
Form 990 Sch B	Schedule B donor disclosure: protect the confidentiality of substantial-donor information regardless of public-disclosure exemption.	Role-based access to the donor database, encryption at rest and in transit, M365 Purview DLP rules on donor-PII patterns, audit log retention.	NO	PART	YES
Form 990 Pt IX	Statement of functional expenses: technology and management costs traceable to mission outcomes for the board and audit committee.	Monthly invoicing by tier, quarterly TBR, vCIO annual written report for the board. Clear allocation between program, management, and fundraising.	YES	YES	YES

STATE CHARITABLE LAW AND BREACH NOTIFICATION - Donor and member PII

State reg.	Charitable solicitation registration in 40+ states; renewals increasingly require attestations about data handling, payment processing, and breach response.	WISP, documented payment processing flow, sub-processor inventory, annual policy review. PTS supplies attestations and evidence binder.	NO	PART	YES
Breach laws	All 50 states require notification of consumers (including donors and members) when PII is breached. Many require AG notification.	Documented IR Plan, breach decision tree, per-state notification scaffolds, cyber insurance activation support, board and AG notification workflow.	NO	NO	YES
PCI DSS v4.0	Donation processing through a credit card brand requires SAQ A or SAQ A-EP at minimum. Annual self-assessment, quarterly external scans where applicable.	Tokenized payment flow, no card data on org systems where possible, documented SAQ, vulnerability scanning, network segmentation guidance.	PART	PART	YES

GRANTOR SECURITY REQUIREMENTS - Federal and foundation flow-downs

Federal grants	Federal grants increasingly flow NIST 800-171-lite or CIS Controls baseline through grant agreements. Some require an SSP and POA&M.	CIS v8.1 IG2 implementation, documented system security plan, plan of action and milestones tracked in vCIO log, evidence binder.	NO	PART	YES
Foundation grants	Major foundations now ask for a WISP, MFA enforcement, backup posture, and incident response plan as part of due diligence.	WISP from PTS policy library, MFA enforcement evidence, monthly air-gapped backup logs, IR Plan with named board liaison.	NO	YES	YES

CIS 01-03 - Inventory of assets, software, and donor data

CIS Control	Requirement	How Guardian Delivers	Co-Mgd	Fund.	Compl.
CIS 01	Inventory and control of enterprise assets connected to the org's infrastructure.	Full asset inventory in a secure documentation portal, M365 device inventory, change-controlled.	YES	YES	YES
CIS 02	Inventory and control of software assets; only authorized software installed and executable.	Software inventory via RMM and centrally managed endpoint policy, application allow-listing on supported endpoints.	PART	YES	YES
CIS 03	Data protection: identify, classify, securely handle, retain, and dispose of donor, member, and payment data.	BitLocker encryption, M365 Purview DLP, encrypted email, documented donor and PII data classification, secure media disposal.	PART	YES	YES

CIS 04-05 - Secure configuration and account management

CIS 04	Secure configuration of enterprise assets and software; patch and update systems.	Documented hardening baselines via Intune and group policy, patch management on supported endpoints, monthly compliance reporting.	YES	YES	YES
CIS 05	Account management: assign and manage credentials for staff, volunteer, board, and service accounts.	M365 identity governance, designated admin accounts, enterprise password vault with rotation, joiner-mover-leaver workflow including volunteer offboarding.	YES	YES	YES

CIS 06-08 - Access control, awareness, audit logging

CIS 06	Access control: phishing-resistant MFA on all remote access, role-based access, quarterly reviews.	Entra ID conditional access, phishing-resistant MFA on email, VPN, RDP, admin, and finance/CRM SaaS via SSO, quarterly access reviews.	YES	YES	YES
CIS 08	Audit log management: collect, alert, review, and retain audit logs.	SIEM with integrated compliance logging, M365 Purview audit log retention, 24/7 MDR, documented monthly log review.	PART	YES	YES
CIS 14	Security awareness and skills training: phishing-resistant culture, social engineering awareness, BEC wire-fraud playbook.	Monthly phishing simulations for staff and board, annual training including BEC red flags, documented completion records.	YES	YES	YES

CIS 11 / 17 - Recovery and incident response

CIS 11	Data recovery: tested practices sufficient to restore in-scope assets to a pre-incident and trusted state.	Image-based cloud backup, monthly air-gapped server backups performed by PTS, monthly restore testing with documented log.	YES	YES	YES
CIS 17	Incident response: documented program to prepare, detect, and respond to attacks.	Documented IR Plan, P1-P4 playbooks, partner SOC threat response, board-ready timeline, annual tabletop exercise, breach notification scaffold.	PART	YES	YES

THE PATH FORWARD

What working with PTS looks like

Four stages, no surprises. Discovery and Assessment within two weeks. Deployed Compliance posture in 30-90 days.

1
Discovery
60-min nonprofit data and CIS readiness review. We map your environment against this document's controls.

2
Assessment
WISP gap and CIS gap assessment. One-page snapshot, policy-library outline, prioritized findings.

3
Implementation
Compliance tier deployed in 30-90 days. M365 E5, SIEM, air-gapped backups, WISP, IR Plan, training.

4
Ongoing
Quarterly TBR, monthly air-gap testing, annual reorientation. Annual written report for the board and audit committee.

Add a vCISO for board-level depth

For orgs facing a federal grant award, a major foundation due-diligence review, a capital campaign launch, or a board cyber inquiry, a fractional **Phantom vCISO** engagement layers on board reporting, compliance roadmap, risk register ownership, and incident liaison. Tiers: Foundation, Operational, Strategic.

Common gaps we find in nonprofits

- MFA on email but not on the donor CRM or finance system
- No WISP or board-ready breach notification scaffold
- Sub-processor inventory missing or last reviewed years ago
- Donor privacy policy copied from a peer, never updated
- Backups exist, but restore testing never performed
- Volunteers and former board members still have access

Important. Nonprofit compliance with IRS Form 990, state charitable solicitation laws, state breach notification laws, PCI DSS, and grantor agreements is the responsibility of the organization and its board. PTS provides the technology, documentation, and program rigor that support those obligations. Final policy adoption, board decisions, and regulatory filings remain with the organization. PTS is not a law firm, an accountancy, or a QSA, and does not provide legal, tax, or PCI assessment advice.

Next step: 30-minute Nonprofit Readiness Review

We walk your environment against this exact mapping and leave you with a one-page gap snapshot. No obligation.

Talk to PTS

hello@phantomts.com
phantomts.com/guardian

Why nonprofits choose Phantom

Since 2010
OPERATING
Indiana-based MSP serving nonprofits, associations, and SMB clients.

100+
POLICY TEMPLATES
WISP and CIS Controls v8.1-aligned policy library applied to every engagement.

24/7
MDR COVERAGE
Partner SOC monitoring, incident response runbooks, board-ready escalation.