# Cybersecurity Policy

## Purpose

This policy provides a foundational cybersecurity framework for Palouse Habitat for Humanity, ensuring the protection of systems, data and stakeholder information. It aligns with the Center for Internet Security, or CIS, Critical Security Controls and the National Institute of Standards and Technology Cybersecurity Framework, or NIST CSF, to establish best practices for cybersecurity.

## Scope

This policy applies to all of Palouse Habitat for Humanity (PHFH), including employees, contractors, volunteers and any third parties who access or manage Habitat information systems, networks and data.

## Governance and risk management

- The Executive Director is responsible for designating a cybersecurity lead responsible for overseeing security efforts.
- The Executive Director will ensure that the Cybersecurity Led will conduct annual risk assessments to identify vulnerabilities and mitigate risks.
- Cybersecurity policies will be reviewed and updated annually or as needed. Any changes impacting the day-to-day workflow of a Habitat representative will be communicated in a timely manner.

## Identity and access management

- Any Habitat representative is required to use multi-factor authentication, or MFA, for all privileged and remote access.
- Role-based access control, or RBAC, will be implemented to ensure users have access only to necessary resources.
- User accounts will be reviewed quarterly, with immediate revocation of access for departing users.
- All Habitat representatives are strongly encouraged to use a different password for each system that requires login.

## Data protection and privacy

- All sensitive data must be encrypted in transit and at rest.
- The Cybersecurity Lead will implement a data classification protocol and enforce appropriate handling measures.
- Regular backups will be conducted and stored securely, with periodic recovery testing.

## Network and endpoint security

- All endpoints will have up-to-date antivirus and endpoint detection and response, or EDR, solutions.
- Networks are segmented to limit access between internal, guest and sensitive systems.
- Firewall and intrusion detection/prevention systems are deployed and monitored.
- To ensure secure access protocols for remote work, all Habitat representatives are required to use the provided virtual private network, or VPN, when connecting to public Wi-Fi or accessing sensitive information.
- All wireless networks must be secured using robust encryption protocols such as WPA3.
- Public Wi-Fi to visitors of Palouse Habitat for Humanity will only be provided securely.

## Secure software development and cloud security

- Cybersecurity Lead will use secure coding practices and conduct security testing before deploying applications.

- Cloud services must comply with security and compliance best practices, including strong access controls.
- Logging and monitoring must be enabled for all critical cloud-based assets.

## Incident response and business continuity

- Palouse Habitat for Humanity will establish incident response plan outlining roles, responsibilities and escalation paths. This plan can be found on PalouseHabitat.org/about under Board Policies and Forms.
- Security incidents must be reported to and investigated promptly by Cybersecurity Lead. Additionally, all cyber incidents/data breaches should be reported to Habitat for Humanity International's cybersecurity team within 48 hours of initial awareness of the incident via the **Habitat Ethics and Accountability Line** or by calling (800) 461-9330. The Cybersecurity Lead is encouraged to work with Habitat for Humanity International's cybersecurity team to contain and triage incidents.
- A business continuity and disaster recovery, or BC/DR, plan is in place and will be tested annually. This plan can be found online at PalouseHabitat.org/about under Board Policies and Forms

## Security awareness and training

- All Habitat representatives accessing sensitive or personal information must complete cybersecurity awareness training quarterly.
- Phishing simulations and security drills will be conducted regularly.
- A culture of security is promoted through this policy and related procedures, with employees being encouraged to report any suspicious activity to the Cybersecurity Lead.

## Vendor and third-party security

- The Cybersecurity Lead will conduct security assessments of vendors and third parties handling Palouse Habitat for Humanity's data.
- Contracts must include security requirements, including incident reporting and compliance obligations.
- Third-party access to Habitat systems must be monitored and limited to necessary services.

## Compliance and audit

- Palouse Habitat for Humanity will comply with applicable federal, state and local cybersecurity regulations.
- Regular audits of information systems and networks will be conducted by the Cybersecurity Lead to ensure adherence to this cybersecurity policy.
- Noncompliance must be addressed with corrective actions and escalation, as needed.

## Continuous improvement

- The Cybersecurity Lead will stay informed on emerging threats and update security practices accordingly.
- Lessons learned from security incidents will be incorporated into policy and process improvements.
- Habitat representatives are encouraged to engage with cybersecurity communities and information-sharing groups on MyHabitat.

## Revision/review history

| Date | Explanation |
|---|---|
| May 5, 2026 | Draft policy approved by consensus vote. |

## Acknowledgment

The Cybersecurity Policy describes important information about Palouse Habitat for Humanity and I acknowledge that I have read and reviewed the requirements contained in the policy and agree that I will follow them.

I also understand that I should consult with my designated Palouse Habitat for Humanity Human Resources, Legal or Information Technology contact regarding any questions not answered in this policy.

_____

Signature

_____

Date received

_____

Name (typed or printed)