

Cybersecurity Policy



Purpose

This policy provides a foundational cybersecurity framework for Chicagoland 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 Chicagoland Habitat for Humanity, including employees, contractors, volunteers and any third parties who access or manage Habitat information systems, networks and data.

Governance and risk management

- The Chief Marketing & Technology Officer is designated as the cybersecurity lead responsible for overseeing security efforts.
- The Chief Marketing & Technology Officer will conduct periodic 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 annually, 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 Chief Marketing & Technology Officer has implemented a data classification policy and will 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 Chicagoland Habitat for Humanity will only be provided securely.

Secure software development and cloud security

- The Chief Marketing & Technology Officer 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

- Security incidents must be reported to and investigated promptly by the Chief Marketing & Technology Officer. 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 Chief Marketing & Technology Officer is encouraged to work with Habitat for Humanity International's cybersecurity team to contain and triage incidents.

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 Chief Marketing & Technology Officer.

Vendor and third-party security

- The Chief Marketing & Technology Officer will conduct security assessments of vendors and third parties handling Chicagoland Habitat for Humanity 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

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

Continuous improvement

- The Chief Marketing & Technology Officer 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
November 12, 2025	Initial policy approved.

FACTS

WHAT DOES CHICAGOLAND HABITAT FOR HUMANITY DO WITH YOUR PERSONAL INFORMATION?

Why?	Financial companies choose how they share your personal information. Federal law gives consumers the right to limit some but not all sharing. Federal law also requires us to tell you how we collect, share, and protect your personal information. Please read this notice carefully to understand what we do.	
What?	<p>The types of personal information we collect and share depend on the product or service you have with us. This information can include:</p> <ul style="list-style-type: none">■ Social Security number and income■ Account balances and payment history■ Credit history and credit scores	
How?	All financial companies need to share customers' personal information to run their everyday business. In the section below, we list the reasons financial companies can share their customers personal information; the reasons Chicagoland Habitat for Humanity chooses to share; and whether you can limit this sharing.	
Reasons we can share your personal information	Does Chicagoland Habitat for Humanity share?	Can you limit this sharing?
For our everyday business purposes— such as to process your transactions, maintain your account(s), respond to court orders and legal investigations, or report to credit bureaus	Yes	No
For our marketing purposes— to offer our products and services to you	Yes	No
For joint marketing with other financial companies	No	We don't share
For our affiliates' everyday business purposes— information about your transactions and experiences	No	We don't share
For our affiliates' everyday business purposes— information about your creditworthiness	No	We don't share
For nonaffiliates to market to you	No	We don't share
Questions?	Call 312-265-6625 or visit us online at chicagolandhabitat.org .	