EMPLOYEE PRIVACY POLICY

Contents

Scope of this Policy

Howard Building Corporation (the "**Company**" or "**we**") has developed this Privacy Policy out of respect for the privacy of our employees and their family members, dependents, and beneficiaries. This Policy describes the personal information we collect, both online and offline, about employees who are employed with us and their family members, dependents, and beneficiaries, for what purposes we use and disclose it, how long we retain it, and whether we sell it or share it for cross-context behavioral advertising purposes (*we don't by the way*).

This Privacy Policy applies only to information collected, used, or disclosed by the Company in the employment context from or about employees and their family members, dependents, and beneficiaries. It does **not** apply to other contexts, such as if you visit our public-facing website or engage in transactions with the Company in other capacities (as a client or customer); interactions outside the employment context are subject to the privacy policy on our website.

Collection of Personal Information and Sensitive Personal Information

In the last 12 months, we have collected the following categories of personal information from or about employees and their family members, dependents, and beneficiaries. For each category of information, we identify below the categories of third parties, service providers, and contractors to whom we have disclosed the information in the last 12 months. The examples provided for each category are not intended to be an exhaustive list or an indication of all specific pieces of information we collect from or about you in each category, but rather the examples are to provide you a meaningful understanding of the types of information that may be collected within each category.

Category	**Personal Identifiers**
Examples	Name, alias, social security number, date of birth, driver's license or state identification card number, passport number, employee ID number
Disclosed in Last 12 Months To	• Financial institutions • Government agencies • Benefits administrators and vendors, including third party administrators, 401K administrators, workers' compensation and unemployment administrators, and wellness vendors • Insurance carriers, administrators, and brokers • Employee tracking and talent management systems • Payroll processors, timekeeping vendors, and vendors providing services for purposes of our human resources information system (HRIS) • Consulting and investigation firms, including human resources consultants, safety consultants • Communications providers • Our corporate customers (meaning an entity, as opposed to a natural person, that purchases, leases, or finances any of our products or services) • Information technology • Affiliated entities (subsidiaries, sister companies)

Category	**Contact Information**
Examples	Home, postal or mailing address, email address, home phone number, cell phone number.
Disclosed in Last 12 Months To	• Financial institutions • Government agencies • Benefits administrators and vendors, including third party administrators, 401K administrators, workers' compensation and unemployment administrators, and wellness vendors • Insurance carriers, administrators, and brokers • Employee tracking and talent management systems • Payroll processors, timekeeping vendors, and vendors providing services for purposes of our human resources information system (HRIS) • Consulting and investigation firms, including human resources consultants, safety consultants • Communications providers • Information technology • Our corporate customers (meaning an entity, as opposed to a natural person, that purchases, leases, or finances any of our products or services) • Affiliated entities (subsidiaries or sister companies)

Category	**Account Information**

Examples	Username and password for Company accounts and systems, and any required security or access code, password, or credentials allowing access to your Company accounts.
Disclosed in Last 12 Months To	• Human resources information system (HRIS)

Category	**Protected Classifications**
Examples	Race, ethnicity, national origin, citizenship or immigration status, sex, gender, sexual orientation, gender identity, religious or philosophical beliefs, age, disability, medical or mental condition, military status, familial status, language, or union membership.
Disclosed in Last 12 Months To	• Government agencies • Benefits administrators and vendors, including third party administrators, 401K administrators, workers' compensation and unemployment administrators, and wellness vendors • Insurance carriers, administrators, and brokers • Employee tracking and talent management systems • Payroll processors, timekeeping vendors, and vendors providing services for purposes of our human resources information system (HRIS) • Consulting and investigation firms, including human resources consultants, safety consultants • Affiliated entities (subsidiaries or sister companies)

Category	**Physical Characteristics or Description**
Examples	Information on your Driver's License (such as eye color, hair color, height, weight), as well as information collected to the extent relevant for workplace investigations or for enforcement of Company policies on appearance and grooming (such as tattoos, piercings).
Disclosed in Last 12 Months To	• Government agencies • Benefits administrators and vendors, including third party administrators, 401K administrators, workers' compensation and unemployment administrators, and wellness vendors • Insurance carriers, administrators, and brokers • Employee tracking and talent management systems • Payroll processors, timekeeping vendors, and vendors providing services for purposes of our human resources information system (HRIS) • Affiliated entities (subsidiaries or sister companies)

Category	**Financial Information**
Examples	Bank account number for direct deposit
Disclosed in Last 12 Months To	• Financial institutions • Government agencies • Payroll processors, timekeeping vendors, and vendors providing services for purposes of our human resources information system (HRIS)

Category	**Internet, Network, and Computer Activity**
Examples	Internet or other electronic network activity information related to usage of Company networks, servers, shared drives, or Company-issued computers and electronic devices, including system and file access logs, browsing history, search history, and usage history.

Disclosed in Last 12 Months To	• Information technology • Affiliated entities (subsidiaries or sister companies)

Category	**Mobile Device Data**
Examples	Data identifying employee's devices accessing Company networks and systems, including cell phone number.
Disclosed in Last 12 Months To	• Payroll processors, timekeeping vendors, and vendors providing services for purposes of our human resources information system (HRIS) • Information technology • Affiliated entities (subsidiaries or sister companies)

Category	**Online Portal and Mobile App Access and Usage Information**
Examples	Username and password, account history, usage history, file access logs.
Disclosed in Last 12 Months To	• Payroll processors, timekeeping vendors, and vendors providing services for purposes of our human resources information system (HRIS) • Information technology

Category	**Visual, Audio or Video Recordings**
Examples	Your image when recorded or captured in pictures of employees taken in the workplace or at a Company function or event, or in pictures or video of employees posted on social media to which the Company or its managers have access or that are submitted to the Company by another employee or third party; recorded calls or meetings, such as recorded Zoom, Teams, or Skype meetings.
Disclosed in Last 12 Months To	• Social media platforms • Office building landlords (for security and access control purposes) • Information technology • Affiliated entities (subsidiaries or sister companies)

Category	**Pre-Hire Information**
Examples	Information provided in your job application or resume, information gathered as part of background screening and reference checks, job interview notes by persons conducting job interviews for the Company, information contained in candidate evaluation records and assessments, information in work product samples you provided, voluntary disclosures by you.
Disclosed in Last 12 Months To	• Payroll processors, timekeeping vendors, and vendors providing services for purposes of our human resources information system (HRIS) • Background check consulting and investigation firms • Affiliated entities (subsidiaries or sister companies)

Category	**Employment History**
Examples	Information regarding prior job experience, positions held, names of prior supervisors, and when permitted by applicable law your salary history or expectations.
Disclosed in Last 12 Months To	• Payroll processors, timekeeping vendors, and vendors providing services for purposes of our human resources information system (HRIS) • Background check consulting and investigation firms • Affiliated entities (subsidiaries or sister companies)

Category	Education Information
Examples	Information from resumes regarding educational history; information obtained from transcripts or records of degrees and vocational certifications obtained.
Disclosed in Last 12 Months To	• Payroll processors, timekeeping vendors, and vendors providing services for purposes of our human resources information system (HRIS) • Background check consulting and investigation firms • Affiliated entities (subsidiaries or sister companies)

Category	Driving Records
Examples	Information contained in your Department of Motor Vehicles record, including traffic violations, convictions, accident history, and departmental actions.
Disclosed in Last 12 Months To	• Background check consulting and investigation firms

Category	Professional or Employment-Related Information
Examples	Information contained in your personnel file and in other employment documents and records, including information contained in the following types of records: new hire or onboarding records, I-9 forms, tax forms, time and attendance records, non-medical leave of absence records, workplace injury records, safety records, performance evaluations and records, disciplinary records, investigatory records, training records, licensing and certification records, compensation and health benefits records, COBRA notifications, business expense records, and payroll records.
Disclosed in Last 12 Months To	• Government agencies • Benefits administrators and vendors, including third party administrators, 401K administrators, workers' compensation and unemployment administrators, and wellness vendors • Insurance carriers, administrators, and brokers • Payroll processors, timekeeping vendors, and vendors providing services for purposes of our human resources information system (HRIS)

Category	Medical and Health Information
Examples	Medical information contained in such documents as doctor's notes for absences or work restrictions, medical leave of absence records, requests for accommodation, interactive process records, ergonomic assessment and accommodation records, and correspondence with you and your medical or mental health provider(s) regarding any request for accommodation or medical leave of absence, as well as information in post-hire drug test results, and information related to symptoms, exposure, contact tracing, diagnosis, testing, or vaccination for infectious diseases (e.g., COVID-19), pandemics, or other public health emergency. This includes medical information and health benefits information for dependents and beneficiaries.
Disclosed in Last 12 Months To	• Government agencies • workers' compensation and unemployment administrators • Insurance carriers, administrators, and brokers • Consulting and investigation firms, including human resources consultants, safety consultants

Category	Family Information
Examples	Contact information for family members listed as emergency contacts, contact information for dependents and other dependent information.
Disclosed in Last 12 Months To	• Payroll processors, timekeeping vendors, and vendors providing services for purposes of our human resources information system (HRIS)

Category	Travel Information
Examples	Dates of business travel or vacation.
Disclosed in Last 12 Months To	• Payroll processors, timekeeping vendors, and vendors providing services for purposes of our human resources information system (HRIS)

Category	Inferences
Examples	Based on analysis of the personal information collected, we may develop inferences regarding employees' preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes for purposes of employment and management decisions related to staffing, assignments, responsibilities, team composition, hiring, promotion, demotion, and termination, among other things.
Disclosed in Last 12 Months To	• Vendors providing services for purposes of our human resources information system (HRIS)

Category	Contents of Personal Communications where the Company is not the intended recipient
Examples	If you use Company email, phones, computers, online chat applications (Teams, Zoom, etc.) or other Company systems for personal communications where the Company is not the intended recipient of the communication, the Company retains these communications in the ordinary course of managing its communication and computer systems and pursuant to the Company's data retention policy. Employees have no expectation of privacy with respect to any communications or data they send, receive, access or store on any company computer or system, including any personal communications. The Company may monitor, access, review and use all such communications and data for lawful business purposes detailed below, including to manage and evaluate employee performance and make employment decisions.
Disclosed in Last 12 Months To	Not Disclosed

What Sensitive Personal Information We Collect

Of the above categories of personal information, the following are categories of sensitive personal information we may collect from or about employees:

1. Personal Identifiers (social security number, driver's license or state identification card number, passport number)
2. Account Information (your Company account log-in, in combination with any required security or access code, password, or credentials allowing access to the account)
3. Protected Classifications (racial or ethnic origin, citizenship or immigration status, religious or philosophical beliefs, union membership, or sexual orientation)

4. Medical and Health Information
5. Contents of Personal Communications (contents of mail, email, and text messages where the Company is not the intended recipient)

Personal information ***does not*** include:

- Publicly available information from government records.
- Information that a business has a reasonable basis to believe is lawfully made available to the general public by the employee or from widely distributed media.
- Information made available by a person to whom the employee has disclosed the information if the employee has not restricted the information to a specific audience.
- De-identified or aggregated information.

Sources of Personal Information

We may collect your personal information from the following sources:

- You, the employee, when you voluntarily submit information for employment purposes
- Company-issued computers, electronic devices, and vehicles
- Company systems, networks, software applications, and databases you log into or use in the course of performing your job, including from vendors the Company engages to manage or host such systems, networks, applications or databases
- physical testing providers and vendors
- HR support vendors, including administrators of benefits, workers' compensation, unemployment claims, payroll, timekeeping, expense management
- Social media platforms
- Background check consulting and investigation firms
- Personal references and former employers
- Our other employees, contractors, vendors, suppliers, guests, visitors, and customers based on your interactions with them
- Affiliated entities (subsidiaries or sister companies)

To Whom We Disclose Personal Information

We may disclose your personal information to the following categories of service providers, contractors, or third parties:

- Financial institutions
- Government agencies
- Benefits administrators and vendors, including third party administrators, 401K administrators, workers' compensation and unemployment administrators, and wellness vendors
- Insurance carriers, administrators, and brokers
- Employee tracking and talent management systems
- Payroll processors, timekeeping vendors, and vendors providing services for purposes of our human resources information system (HRIS)
- Consulting and investigation firms, including human resources consultants, and safety consultants
- Communications providers/vendors
- Social media platforms
- Background check consulting and investigation firms

- Our corporate customers (meaning an entity, as opposed to a natural person, that purchases, leases, or finances any of our products or services)
- Information technology
- Affiliated entities (subsidiaries or sister companies)

Reasons Why We Collect, Use, Retain, and Disclose Personal Information

We may collect, use, and disclose your personal information for any of the following business purposes:

1. To fulfill or meet the purpose for which you provided the information. For example, if you share your name and contact information to become an employee, we will use that Personal Information in connection with your employment.
2. To comply with local, state, and federal law and regulations requiring employers to maintain certain records (such as immigration compliance records, travel records, personnel files, wage and hour records, payroll records, accident or safety records, and tax records).
3. To manage and process payroll and/or Company travel and expenses.
4. To validate an employee's identity for payroll and timekeeping purposes.
5. To maintain commercial insurance policies and coverages, including for workers' compensation and other liability insurance.
6. To manage workers' compensation claims.
7. To manage employee performance of their job duties and/or employee conduct, including by engaging in lawful monitoring of employee activities and communications when they are on duty, on Company premises, or utilizing Company internet and WiFi connections, computers, networks, devices, software applications or systems.
8. To conduct workplace investigations (such as investigations of workplace accidents or injuries, harassment, or other misconduct).
9. To obtain and verify background checks on job applicants and employees and to verify employment references.
10. To communicate with employees regarding employment-related matters such as upcoming benefits enrollment deadlines, action items, availability of W2s, and other alerts and notifications.
11. To grant employees access to secure Company facilities and maintain information on who accessed the facility.
12. To engage in marketing efforts on behalf of the Company.
13. To track and record sales and other transactions with our customers.
14. To implement, monitor, and manage electronic security measures on Company internet and WiFi connections, computers, networks, devices, software applications or systems, as well as on employee devices that are used to access Company internet and WiFi connections, computers, networks, devices, software applications or systems.
15. To engage in corporate transactions requiring review or disclosure of employee records subject to non-disclosure agreements, such as for evaluating potential mergers and acquisitions of the Company.
16. To communicate with an employee's family or other contacts in case of emergency or other necessary circumstance.
17. To manage employee recognition programs.
18. To promote and foster diversity, equity, and inclusion in the workplace.
19. To remain competitive in offering a variety of special discounts and benefits to employees.
20. To comply with our contractual obligations.
21. To provide services to corporate customers who may request certain pieces of information about a Company employee (such as name, phone number, and headshot) to permit the employee access or security clearance to their facility in advance of the Company employee being dispatched to provide services at the customer's facility.
22. Infectious disease purposes (pandemic, outbreak, public health emergency, etc.)

23. To evaluate, assess, and manage the Company's business relationship with vendors, service providers, and contractors that provide services to the Company.
24. To improve user experience on Company computers, networks, devices, software applications or systems, and to debug, identify, and repair errors that impair existing intended functionality of our systems.
25. To detect security incidents involving potentially unauthorized access to and/or disclosure of Personal Information or other confidential information, including proprietary or trade secret information and third-party information that the Company received under conditions of confidentiality or subject to privacy rights.
26. To protect against malicious or illegal activity and prosecute those responsible.
27. To prevent identity theft.
28. To verify and respond to consumer requests under applicable consumer privacy laws.

We do <u>NOT</u> and will not sell your personal information in exchange for monetary or other valuable consideration. We do not share your personal information for cross-context behavioral advertising.

We do <u>NOT</u> and will not use or disclose your sensitive personal information for purposes other than the following:

1. To perform the services reasonably expected by an average employee who requests those services.
2. To ensure the physical safety of natural persons.
3. For purposes that do not involve inferring characteristics about the consumers.

Retention of Personal Information

We will retain each category of personal information in accordance with our established data retention policy and practice. In deciding how long to retain each category of personal information that we collect, we consider many criteria, including, but not limited to: the business purposes for which the Personal Information was collected; relevant federal, state and local recordkeeping laws; applicable statute of limitations for claims to which the information may be relevant; and legal preservation of evidence obligations.

We apply our data retention procedures on an annual basis to determine if the business purposes for collecting the personal information, and legal reasons for retaining the personal information, have both expired. If so, we will purge the information in a secure manner.

Third-Party Vendors

We may use other companies and individuals to perform certain functions on our behalf. Examples include administering e-mail and payroll services. Such parties only have access to the personal information needed to perform these functions and may not use or store the information for any other purpose.

Business Transfers

In the event we sell or transfer a particular portion of our business assets, employee information may be one of the business assets transferred as part of the transaction. If substantially all of our assets are acquired, employee information may be transferred as part of the acquisition.

Compliance With Law and Safety

We may disclose specific personal and/or sensitive personal information based on a good faith belief that such disclosure is necessary to comply with or conform to the law or that such disclosure is necessary to protect our employees or the public.

Employees and Their Family Members, Dependents, and Beneficiaries Under the Age of 16

We do **not** knowingly sell or share the personal information of employees or any of their family members, dependents or beneficiaries under 16 years of age.

How We Protect the Information That We Collect

The protection of the information that we collect about employees is of the utmost importance to us and we take every reasonable measure to ensure that protection, including:

- We keep automatically collected data and voluntarily collected data separate at all times.
- We use internal encryption on all data stores that house voluntarily captured data.
- We use commercially reasonable tools and techniques to protect against unauthorized access to our systems.
- We restrict access to private information to those who need such access in the course of their duties for us.

Rights Under the CCPA and CPRA

This section of the Privacy Policy applies only to California residents. If you are a California resident, you have the following rights pursuant to the California Consumer Privacy Act (CCPA) as amended by the California Privacy Rights Act (CPRA):

1. Right to Know. The right to request, up to 2 times in a 12-month period, that we identify to you (1) the categories of personal information we have collected, shared or sold about you, (2) the categories of sources from which the personal information was collected, (3) the business purpose for which we use this information, and (4) the categories of third parties with whom we disclose or have disclosed your personal information;

2. Right to Access. The right to request, up to 2 times in a 12-month period, that we provide you access to or disclose to you the specific pieces of personal information we have collected about you;

3. Right to Delete. The right to request, up to 2 times in a 12-month period, that we delete personal information that we have collected from you, subject to certain exceptions;

4. Right to Correct. The right to request that we correct inaccurate personal information (to the extent such an inaccuracy exists) that we maintain about you;

5. The right to designate an authorized agent to submit one of the above requests on your behalf. See below for how you can designate an authorized agent; and

6. The right to not be discriminated or retaliated against for exercising any of the above rights.

How to Submit Requests:

You can submit any of the above types of requests by email at: **hr@howardbuilding.com**

How We Will Verify That it is Really You Submitting the Request:

If you are a California resident, when you submit a Right to Know, Right to Access, Right to Delete, or Right to Correct request through one of the methods provided above, we will ask you to provide some information in order to verify your identity and respond to your request. Specifically, we will ask you to verify information that can be used to link your identity to particular information in our possession, which depends on the nature of your relationship and interaction with us.

Responding to your Right to Know, Right to Access, Right to Delete, and Right to Correct Requests

Upon receiving a verifiable request from a California resident, we will confirm receipt of the request no later than 10 business days after receiving it. We endeavor to respond to a verifiable request within forty-five (45) calendar days of its receipt. If we require more time (up to an additional 45 calendar days, or 90 calendar days total from the date we receive your request), we will inform you of the reason and extension period in writing. We will deliver our written response by mail or electronically, at your option. The response we provide will also explain the reasons we cannot comply with a request, if applicable.

We do not charge a fee to process or respond to your verifiable request unless it is excessive, repetitive, or manifestly unfounded. If we determine that the request warrants a fee, we will tell you why we made that decision and provide you with a cost estimate before completing your request.

For a request to correct inaccurate personal information, we will accept, review, and consider any documentation that you provide, and we may require that you provide documentation to rebut our own documentation that the personal information is accurate. You should make a good-faith effort to provide us with all necessarily information at the time that you make the request to correct. We may deny a request to correct if we have a good-faith, reasonable, and documented belief that a request to correct is fraudulent or abusive. If we deny your request to correct, we shall inform you of our decision not to comply and provide an explanation as to why we cannot comply with a request, if applicable.

If You Have an Authorized Agent:

If you are a California resident, you can authorize someone else as an authorized agent who can submit a request on your behalf. To do so, you must either: (a) execute a valid, verifiable, and notarized power of attorney; or (b) provide other written, signed authorization that we can then verify. When we receive a request submitted on your behalf by an authorized agent who does not have a power of attorney, that person will be asked to provide written proof that they have your permission to act on your behalf. We will also contact you and ask you for information to verify your own identity directly and not through your authorized agent. We may deny a request from an authorized agent if the agent does not provide your signed permission demonstrating that they have been authorized by you to act on your behalf.

Consent to Terms and Conditions

By entering into an employment relationship with Howard Building Corporation, you consent to all terms and conditions expressed in this Privacy Policy.

Changes to Our Privacy Policy

As our services evolve and we perceive the need or desirability of using personal information collected in other ways, we may from time to time amend this Privacy Policy. We encourage you to check the Employment Privacy Policies folder on SharePoint frequently to see the current Privacy Policy in effect and any changes that may have been made to them. If we make material changes to this Policy, we will post the revised Policy and the revised effective date in the Employment Privacy Policies folder on SharePoint. Please check back here periodically or contact us at the address listed at the end of this Policy.

Individuals With Disabilities

This Policy is in a form that is or will be made accessible to individuals with disabilities.

Questions About the Policy

If you have any questions about this Privacy Policy, please contact us by email at **hr@howardbuilding.com** or call **(213) 683-1850.**

*****This Policy was last updated September 30, 2025.***