Acuity International Employee Privacy Notice
Last updated August 12, 2026

This Employee Privacy Notice ("**Privacy Notice**") describes the collection, use, retention, and sharing of your personal information through the course of your tenure with Acuity International (" **Acuity**", "**we**", "**us**", "**our**") and its subsidiaries and affiliates. For additional information on our general privacy practices, please see our Privacy Notice.

APPLICABILITY

This Privacy Notice applies to personal information, which is information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household, collected from personnel of Acuity. The term " **personnel**" includes current employees and those that work on a non-permanent basis, such as temporary workers that are assigned to us through a temporary staffing agency.

PERSONAL INFORMATION WE COLLECT, WHY AND FOR HOW LONG

During the course of your tenure with Acuity, we collect personal information about you, as well as personal information related to your dependents and beneficiaries (collectively, "**Dependents**"), where there is a legitimate reason to do so in connection with our relationship with you. To the extent we collect personal information on your Dependents, you should inform your Dependents that you are providing this information to us and why, and make sure that it is acceptable to them.

Through your tenure with Acuity, Acuity will collect personal information to:

- **Administer salary and benefits.** We collect, from you, as well as from governmental entities, and benefit providers your *personal identifiers* (name, telephone number, physical address, email address, date of birth, signature), your *sensitive personal identifiers* (Social Security number, driver's license number, state identification number, and passport (if provided)), your *financial information* (bank account and routing number, salary information, withholding tax and insurance information), and your *employment information* (level of employment, position, role, tasks, certifications, workspace, etc.). Social Security number, driver's license number, state identification number, and passport are considered sensitive under the California Consumer Protection Act, as amended ("CCPA"). We use this information to administer payroll and employee benefit plans, including enrollment and claims handling. We also collect, from you, the *personal identifiers* (name, date of birth) and *sensitive personal identifiers* (Social Security number) of Dependents. We use the Dependent information to process their eligibility as your Dependents for the purpose of benefits. We retain data related to compensation, benefit, and retirement plans indefinitely pursuant to legal reporting requirements.

- **Conduct employee onboarding**. When you first join Acuity, we collect, from you, your *pe rsonal identifiers* (name, telephone number, physical address, email address, date of birth, signature), your *sensitive personal identifiers* (Social Security number, driver's license

number, state identification number, and passport (if provided)), your *protected classifications* (marital status, age, gender, disability status (if provided), veteran status (if provided)), your *sensitive protected classifications* (race, ethnicity, (if provided)), and your *financial information* (bank account and routing number, salary information, withholding tax and insurance information). We use this information to onboard you as an employee of Acuity. We use this protected classification and sensitive protected classification information for government reporting purposes, to comply with legal requirements, to analyze requested disability accommodations as applicable, and to document any accommodations we have provided to accommodate your needs. We also collect, from you, the *personal identifiers* (name, telephone number, email address, physical address) of your emergency contacts to communicate with these contacts in the event of an emergency. We use this information, in the aggregate, to conduct internal analytics and benchmarking.

- **Create a personnel file.** When you first join Acuity and throughout your tenure with us, we collect, from you, your *personal identifiers* (name, date of birth, telephone number, physical address) and *professional information* (licenses, credentials, employment history, educational history, resume/CV, disciplinary evaluations, performance reviews, terms and conditions of employment, salary (including retirement accounts, pensions, or insurance coverage), skills, qualifications, experience, travel history, professional/occupational memberships, and time-off work). We use this personal information to maintain your personnel file, create personnel biographies, and for internal recruitment purposes (assessing your eligibility for other positions within Acuity. We retain this information up to seven (7) years after separation from Acuity.

- **Manage business and travel expenses.** When you travel in connection with your tenure with Acuity, we collect, from you or from our travel and expense management service provider, your *personal identifiers* (name, phone number, email address, country), *corporate financial information* (travel and expense details, cost center), and the *personal identifiers* (name) of your manager. We use this information to manage business and travel expenses incurred during the course of your tenure.

- **Process workers' compensation and health insurance claims**. If you file a workers' compensation or health insurance claim, we collect, from you, your *personal identifiers* (name), your *medical information* (job restrictions, workplace illness, injury information) and your *sensitive personal information* (health information). We use this information to investigate and process workers' compensation claims, arrange for health insurance benefits and to conduct and process employment testing. We retain this information in accordance with state and federal medical records laws.

- **Professional development**. We collect, from you, your *personal identifiers* (name) and *professional information* (licenses, credentials, employment history, educational history, resume/CV, disciplinary evaluations, performance data, training data). We use this information to identify, deliver, and track training needs and outcomes, to help with career development, succession planning, and workforce management and to manage professional requirements, certifications and memberships and to manage relationships with vendors. We retain this information for seven (7) years after separation.

- **Conduct IT security and management.** When you access our computer network, information systems, digital assets, or use Acuity-owned electronic devices, we collect, from you, your *personal identifiers* (username, IP address, device identifiers), your *electronic network activity information* (logins, accesses, browsing history, search history, websites visited, interactions with websites), and your *sensitive personal information* (password). We use this information to ensure compliance with Acuity's policies and procedures, to protect Acuity's computer network, for authentication purposes, to provide IT support, and to prevent loss of Acuity property. When you log into our computer network, we also collect your *geolocation data* (country or city and state) automatically through an analytics solution to confirm the login is associated with a known location.

- **Assess performance at work.** Throughout your tenure with Acuity, we collect, from you, your *personal identifiers* (name) and *employment information* (skills, working hours and achievement of set goals). We use this to: (i) conduct performance reviews; (ii) issue probation reviews and professional development reviews; (iii) maintain disciplinary measures; (iv) verify compliance and effectiveness; and (v) ensure employee productivity and adherence to Acuity's policies.

- **Handle general human resources functions.** Throughout your tenure with Acuity, we collect, from you, your *personal identifiers* (name, personnel ID, email address, telephone number, physical address) and emergency contact information. We use this information to handle general human resources functions, such as communication, personnel development, performance management, promotions and succession planning, internal communication and management of industrial relations, personnel surveys, mobility management including international assignment and personnel travel administration, appraisal/review, accounting, attendance and absence management, administration of sick leave, administration of annual leave, promotions, transfers, secondments, creating internal personnel directories, termination, and emergency contact procedures.

- **Process your vacation and leave**. If you take a vacation or leave, we collect, from you, your *personal identifiers* (name, physical address), your *sensitive personal identifiers* (Social Security number), your *medical information* (health status, doctor's notices, accident reports, birth announcement), *protected classifications* (disability details, disability of Dependents), *employment information* (work time information, holiday information, employment position/role, leave of absence information including religious, military and family obligations). We use this information to process your leave or vacation.

- **Issue tax forms.** Throughout your tenure with Acuity, we collect, from you, your *personal identifiers* (name, physical address), your *sensitive personal identifiers* (Social Security number) and your *tax information* (withholding details). We use this information to issue tax forms and comply with tax reporting requirements. We retain this information up to seven (7) years after separation.

- **Evaluate need for reasonable accommodations**. If you request reasonable accommodations, we collect, from you, your *personal identifiers* (name, email address, telephone number, physical address), your *medical information* (doctor's notes, requests

for accommodations) and your *protected classifications* (religious or philosophical beliefs, any disabilities you may have). We use this information to evaluate, upon request, the need such accommodations and to process them.

- **Comply with legal obligations.** Throughout your tenure with Acuity, we collect, from you, as well as from benefits providers, governmental entities, and background check providers, your *protected classifications* (ethnicity, nationality, citizenship status, gender, military or veteran status (if provided), any disabilities you may have (if provided)). We use this information to comply with our obligations under applicable state and federal labor laws, employment laws, equal opportunity and anti-discrimination laws, workers' compensation laws, workplace safety laws, tax benefits laws and related laws.

- **On-site Security.** When you attend our on-site facilities, we utilize CCTV cameras and therefore collect, automatically, video of you through our CCTV cameras. We use this information to maintain the safety and security of our employees, clients, and facilities.

- **Aggregate data.** We aggregate the data we collect for benchmarking purposes and for internal analytics.

Acuity will also use the personal information we collect as described in this section to comply with the law, to efficiently maintain our business, and for other limited circumstances as described in **HOW WE SHARE YOUR PERSONAL INFORMATION.**

We process your personal information for as long as our processing purposes, the legal retention periods and our legitimate interests in documentation and keeping evidence or when storage is a technical requirement as set forth in our records retention policy. If there are no contrary legal or contractual obligations, we will delete or anonymize your data once the storage or processing period has expired as part of our usual processes. We may need to use and retain your personal information for longer than these reasons for purposes of:

- *Compliance with our legal obligations*. For example, retaining your employee records the purpose of accounting, dispute resolution and compliance with labor, tax and other financial regulations.
- *Meeting our safety and security commitments*. Such as keeping our properties secure and preventing fraud.
- *Exercising or defending legal claims*. We also may need to retain information for longer than the terms in order to meet with legal process or enforceable governmental request, or to enforce our employment agreements including investigation of potential violations.

HOW WE SHARE YOUR PERSONAL INFORMATION

A. General Sharing

We share your personal information as follows:

- **Within Acuity.** We share personnel personal information within Acuity to receive IT services/security, Human Resources, tax and accounting, payroll, and general business and employment management. Access to personal information is limited to those on a need-to-know basis.

- **With Service Providers.** We share your personal information with our service providers to assist us in managing and administrating your tenure. These service providers include providers of payroll, enterprise human capital management software, financial services, employee compensation management services, employee travel and expense management services, insurance, health benefits, human resources services, IT systems and support, and similar providers engaged to assist us in carrying out business activities and HR-related functions.

- **For legal purposes**. We share personal information where we are legally required to do so, such as in response to court orders, subpoenas, governmental/regulatory bodies, law enforcement or legal process, including for national security purposes. We may share your information with our legal advisors or auditors to establish, protect, or exercise our legal rights or as required to enforce our terms of service or other contracts or to defend against legal claims or demands. We also share this information with third parties as necessary to: detect, investigate, prevent, or take action against illegal activities, fraud, or situations involving potential threats to the rights, property, or personal safety of any person; to comply with the requirements of any applicable law; or to comply with our legal obligations.

- **During a corporate reorganization.** In the event that we enter into, or intend to enter into, a transaction that alters the structure of our business, such as a reorganization, merger, acquisition, sale, joint venture, assignment, consolidation, transfer, change of control, or other disposition of all or any portion of our business, assets or stock, we will share personnel personal information. We will also share personal information with third parties if we undergo bankruptcy or liquidation, in the course of such proceedings.

- **With your consent**. Apart from the reasons identified above, we may request your permission to share your personal information for a specific purpose. We will notify you and request consent before you provide the personal information or before the personal information you have already provided is shared for such purpose. You may revoke your consent at any time and may do so by contacting us via email at humanresources@acuityinternational.com.

B. <u>Sharing in the Preceding Twelve (12) Months</u>

For Business Purposes. In the preceding twelve (12) months, Acuity has disclosed the following categories of personal information for a business purpose to the following categories of third parties:

- We have disclosed your personal identifiers, protected classifications, professional or employment related information, internet or other electronic network information, and your customer records information to service providers that help us perform employment-related functions. These service providers include IT support, background check companies, payroll processors, compensation management providers, expense processors, health insurance providers, and benefits providers.

- We have disclosed your personal identifiers and internet or other electronic network information to IT support to detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity, to identify and repair errors that impair functionality, and to improve, upgrade, or enhance Acuity devices.

C. <u>Sale of Personal Information</u>

Acuity does not sell personnel personal information, nor does it share this information with third parties for cross-context behavioral advertising (i.e. targeted advertising).

RIGHTS OF CALIFORNIA EMPLOYEES

The California Consumer Privacy Act of 2018, as amended ("**CCPA**"), entitles California residents to certain rights. If our processing of your personal information is subject to the CCPA, you are entitled to the following rights:

- **Right to Access/Know.** You have the right to request what personal information we have collected, used, disclosed, and sold about you, unless doing so proves impossible or would involve disproportionate effort. You may make two free requests for access within a 12-month period.

- **Right to Deletion.** You have the right to request the deletion of your personal information that we collect or maintain, subject to certain exceptions. For example, if we are required by law to retain the information that you are asking to be deleted, we would not be able to delete the information until we are legally permitted to delete it.

- **Right to Correct.** You have the right to correct inaccurate personal information that we collect or maintain.

- **Right to Opt Out of Sale/Sharing.** We do not sell personnel personal information or share this information with third parties for targeted advertising purposes.

- **Right to Non-Discrimination (Non-Retaliation in California).** You have the right to not receive discriminatory treatment if and when you exercise your rights under the CCPA.

- **Right to Limit Use of Sensitive Personal Information.** You have the right to limit the use of your sensitive personal information when such use goes beyond that which is necessary for providing the Services or certain other permissible purposes like fraud, customer service or quality control. Sensitive information includes Social Security number, driver's

license number, biometric information, precise geolocation, and racial and ethnic origin. However, Acuity does not process sensitive personal information in a manner which gives rise to this right.

To exercise your privacy rights, you may submit a request by emailing us at humanresources@acuityinternational.com or by contacting us toll-free at 800-868-8500 and ask for Human Resources.

For requests submitted via telephone, you must provide us with sufficient information that allows us to reasonably verify you are the person about whom we collected the personal information and describe your request with sufficient detail to allow us to properly evaluate and respond to it. In doing so, we will take steps to verify your request by matching information provided by you with the information we have in our records. If we are not able to verify your identity for access and deletion requests with the information provided, we may ask you for additional pieces of information.

Only you, or a person that you authorize to act on your behalf may make a request related to your personal information. If you are an authorized agent making a request on behalf of another individual, you must provide us with signed documentation that you are authorized to act on behalf of that individual.

RIGHTS OF ALL EMPLOYEES

Regardless of your state of residence, you may be entitled to certain rights under applicable labor laws. For more information, please email us at humanresources@acuityinternational.com and include "Labor Law Inquiry" in the subject line.

INFORMATION SECURITY

We implement appropriate technical and organizational security measures, such as access controls and encryption and 24-7 threat monitoring, to protect the personal information that we collect and maintain from unauthorized access, destruction, use, modification, or disclosure. However, no security measure or modality of data transmission is 100% secure, and we are unable to guarantee the absolute security of the personal information we have collected from you.

CHANGES TO THIS PRIVACY NOTICE

This Privacy Notice is not part of a contract of employment with you. Acuity reserves the right to update or modify this Privacy Notice in our sole discretion at any time without prior notice. If we do, we will post the changes to this site and will indicate the date the changes go into effect. We encourage you to review our Privacy Notice to stay informed. If we make changes that materially affect your privacy rights, we will notify you by prominent posting on Acuity's intranet, and obtain your consent, if required.

CONTACT US

If you have any questions about this Privacy Notice or need to access this Privacy Notice in an alternative format due to having a disability, please contact us via email at humanresources@acuityinternational.com or call us toll-free at 800-868-8500 and ask for Human Resources.