IMPETUS

Privacy Policy

Responsibilities

The information in our records must be accurate and up to date. If personal information changes during employment, the user must inform the company.

The company endeavors to maintain physical, technical, and procedural safeguards appropriate to the sensitivity of personal information. These safeguards prevent personal information from being lost, accessed without authorization, copied, used, modified, or disclosed.

Introduction

The company is committed to maintaining the accuracy, confidentiality, and security of personal information. This privacy policy outlines the personal information the company collects from various sources, how it is used, and to whom it is disclosed.

The company has a designated grievance officer responsible for promptly addressing grievances. The standard response time is within 30 days of receiving a grievance.

Details of Grievance Officer

The Company has appointed a grievance officer who can be contacted for any privacy-related events

Name: Abhishek Kumar Singh

Designation: Senior Director HEG

Email: privacy@impetus.com

Personal information type

The company may collect personal information from various sources, which includes

Employment purpose: The company may collect and maintain different types of personal information from individuals who seek to be, are, or were employed by us, including but not limited to:

- Resumes and/or applications
- References and interview notes
- Photographs and videos
- Medical records and history
- Biometric information
- Letters of offer and acceptance of employment
- Mandatory policy acknowledgment sign-off sheets
- Payroll information
- Beneficiary and emergency contact information
- Details provided to the company for service-related purposes

In addition to the examples listed above, personal information includes details such as name, home address, telephone number, personal email address, date of birth, employee identification number, marital status, and any other information necessary for business purposes that an employee voluntarily discloses during the employment application process.

Any information that is freely available or accessible in the public domain will not be treated as sensitive personal data.

The company also collects information through its websites and other marketing and sales activities. Information collected through these activities is used solely for relevant business purposes. By accessing the company's websites and platform, the user agrees to the company's data usage policies.

The company ensures that individuals are informed about the specific data being collected and the purpose for which it is used.

Usage of personal information

The personal information collected is used and disclosed for our business purposes, including establishing, managing, or terminating your employment with the company. Such uses include:

- Determining eligibility for initial employment, including the verification of references and qualifications
- Improving the services or platforms, such as websites
- Sales and marketing information
- Administering pay and benefits
- Processing employee work-related claims (e.g., workers' compensation, insurance claims, etc.)
- Assessing qualifications for a particular job or task
- Gathering evidence for disciplinary action or termination
- Establishing a contact point in the event of an emergency (such as next of kin)
- Ensuring the security of company-held information
- Any other purposes reasonably required by the company

Monitoring

The work output of company employees—whether in paper records, computer files, or any other storage format—belongs to the company. This work output, along with the tools used to generate it, is always subject to company review and monitoring.

While conducting business, we may monitor employee activities, as well as our premises and property. For example, some locations are equipped with surveillance cameras to protect employees and third parties from theft, vandalism, and property damage.

In accordance with our policies, such as the Acceptable Use Policy, IT Infrastructure Use Policy, and Internet Access Policy, we may monitor employees' computer and email usage.

To protect the company's intellectual property, monitoring and surveillance tools, such as screen capturing and/or key loggers, may be used with company-owned resources. Users are required not to use these resources for personal access, data storage, or any unauthorized transfer. The company may reclaim such resources to analyze stored and used data. Users must release the resource immediately upon request by IT personnel.

This does not imply that all employees are monitored or subject to constant surveillance. Rather, it is intended to inform you that such monitoring may occur and could result in the collection of personal information from employees (e.g., through their use of company resources). When using company equipment or resources, employees should not expect privacy regarding their usage.

Personal information disclosure

We may share your personal information with our employees, contractors, customer consultants, and other parties who require this information to establish, manage, or terminate our employment relationship. This may include parties that provide products or services to us or on our behalf and those who collaborate with us to provide products or services to you.

Furthermore, your personal information may be disclosed for reasons including, but not limited to:

- As permitted or required by applicable laws or regulatory requirements.
- To protect the rights and property of the company.
- During emergencies or when necessary to protect the safety of an individual or a group.
- To third parties for background screening.
- We will endeavor not to disclose more personal information than required in such cases.

Notification and consent

To the extent that your consent is required, we will assume—unless you advise us otherwise—that by using the systems and resources, you have consented to the company collecting, using, and disclosing your personal information for the purposes necessary for that collection.

If an individual disagrees with data collection, they should immediately stop using the data and inform the company.

The information provider may also withdraw their consent for data usage; in such cases, the company will choose not to provide the services.

Upon request, the company will provide access to review the information, and any data found to be inaccurate or reported as deficient will be corrected or amended.

The organization is not responsible for the authenticity of data collected or supplied by the information provider.

Information retention

The company retains the information, except as otherwise permitted or required by applicable law or regulatory requirements, only for as long as necessary to fulfill the purposes for which it was collected.

Security Measures and Protection

Impetus is an ISO 27001-certified organization committed to maintaining a security infrastructure and practices in line with the standard.

Impetus maintains a comprehensive information security program and maintains technical, physical, and operations security controls.

An incident response program is in place to notify stakeholders about any security incidents involving data breaches.