



PRIVACY STATEMENT

Your privacy is important to us. This Privacy Statement provides how the personal information you provided or we collected will be used and managed. We respect and value the personal information you entrusted us and we will abide by the spirit and principles of the Data Privacy Act of 2012.

As a condition for availing of our services, you are agreeing to this Privacy Statement of the Metals Industry Research and Development Center and to the collection, use, storage, retention and destruction, access, disclosure and sharing of your personal information as described in this Privacy Statement.

This Privacy Statement applies to all the services the Center offers.

Collection

[What personal information do we collect and hold?](#)

Depending on the official transaction involved, we may collect the following types of personal information:

- identification details, such as your name, age or birth date, civil status, gender, signature, photo;
- contact details, such as your residential or business address, email address, telephone number (work and home) or facsimile number;
- personal information contained in any emails entering and exiting our server; and
- unique identifiers, such as your government issued identification card

In addition, in compliance with government issuances:

- if you are a job applicant --- the Personal Data Sheet requires you to fill in your family background, ethnic origin, religion, educational background, employment information, voluntary works or involvement in civic/non-government/people/voluntary organizations; political or organizational affiliations, parental status; legal liabilities in any administrative or criminal proceedings, or conviction of any crime or violation of any laws by any court or tribunal;
- if you are a supplier or contractor – banking and financial details, such as your bank account details, financial statements, tax returns, licenses or permits;
- if you are hired as a new employee, a contract of service or job order – biometrics, health information, such as medical history, drug screen results, blood group details, medications, visual acuity, physical examination; and

- if you are an applicant for a technology license --- education, government issued licenses or its denials, suspension or revocation, tax returns, current position/designation at work, affiliation with other business and organizational affiliations.

How do we collect your personal information?

Our frontline receiving personnel collects your personal information directly from you unless it is unreasonable or impracticable to do so. We collect personal information from you in the following ways:

- during discussions between you and our frontline personnel prior to engagement of our services;
- when you participate in the procurement activities of the Center;
- when you or someone else sends us your resume/curriculum vitae or personal data sheet (PDS);
- when you complete/accomplish one of our forms or avail of any of our services, submit an application, sign in or register as a visitor or researcher;
- through incident and internal investigations; and
- when you access and use our online presence.

We may also collect personal information from third parties, such as your employer (current and previous), universities and other educational institutions, your references as listed in your resume, and other DOST agencies or government and private entities.

Use

For what purposes do we collect, hold, use and disclose your personal information?

We collect personal information from you to comply with the relevant law and statutes, to fulfill the Center's mandate and to provide the best possible quality of services to our stakeholders.

We collect, hold, use and disclose your personal information for the following purposes:

- to establish communications with you, such as answering inquiries and providing information or advise about the technical services we offered, or to inform you of the status of your service request;
- to update our records/database and keep your contact details up to date;
- to process your service request, job application or billing statements; and
- to assess your qualifications for availing our technology-based programs, such as training, consultancy and technology transfer;

Storage, Retention and Destruction

How do we store your personal information?

We may store your personal information in documentary or electronic form. We will exercise physical security on those documents and electronic versions of the data contained therein. We will also take reasonable steps to destroy or permanently de-identify any personal information that is no longer needed for the purpose for which we collected it or for the purpose of meeting legal requirements. Documents will be kept secure in locked filing cabinets or in locked offices and electronic versions of personal information will be kept secure in password-protected computer files.

How do we retain or dispose of your information?

We have a Central Records Office that manage documented information in accordance with the rules and regulations on retention and disposal of public records prescribed by the National Archives of the Philippines. Your electronically stored personal information in our database will be permanently stored or retained for a specific duration of time prior to deletion as approved by the designated responsible authority.

Access

Who may access your personal data and for what purpose?

Only the customer and the authorized personnel of the Agency shall be allowed to access personal information, except for purposes contrary to law, public policy, public order or morals.

How can you access and correct your personal information?

You may request access to your personal information at any time, subject to any relevant legal requirements and exemptions, including identity verification procedures. As a prerequisite, we will ask for proof of identity and other relevant information as a security measure prior to locating and allowing data access.

In case that certain personal information we possess are deemed incorrect, incomplete or inaccurate, you may request us to amend it by sending us an email at mirdc@mirdc.dost.gov.ph or through a written request to the attention of our Data Protection Officer, Metals Industry Research and Development Center, Gen. Santos Avenue, Bicutan, Taguig City. Data updates or corrections to your personal information will be free of charge.

Disclosure and Sharing

To whom may we disclose your information?

We do not share personal information with other government agencies, companies, organizations and individuals outside of MIRDC unless one of the following circumstances applies:

With your consent. We will share personal information with other government agencies, companies, organizations or individuals outside of the MIRDC when we have your consent to do so. We will require your consent before sharing any of your *sensitive personal information*.

For legal compliance. We may provide personal information in accordance with approved guidelines to other DOST Agencies or government entities to comply with the relevant law or statutes.

For legal reasons. We may also share your personal information with other government entities, organizations or individuals outside of the MIRDC if we believe that disclosure of the information is necessary for legal reasons.

Security Measures

How do we secure your personal information?

To prevent unauthorized access or disclosure and to ensure the appropriate use of your information, we implement organizational, technical and physical security measures to safeguard the information we collect and process.

For example:

- Organizational Security Measures
 - Appointment of Data Protection Officer who shall oversee the compliance of the MIRDC with the DPA, its IRR, and other related policies, including the conduct of a Privacy Impact Assessment, implementation of security measures, security incident and data breach protocol, and the feedback and complaints procedure.
 - Conduct of trainings or seminars to keep personnel, especially the Data Protection Officer updated vis-à-vis developments in data privacy and security.
 - Documented procedures on control of document information are in place and are reviewed for adequacy and effectiveness.

- Physical Security Measures
 - All personal data being processed by the MIRDC shall be stored in a storage/data room, where paper-based documents are kept in locked filing cabinets while the digital/electronic files are stored in computers provided and installed by the Agency where access is protected by a password.
 - Only authorized personnel are allowed access to the storage/data room.

- Technical Security Measures
 - The MIRDC has installed a firewall in all its servers to prevent unauthorized access to our data.
 - MIRDC shall first and evaluate review software applications before the installation thereof in computers and devices of the MIRDC to ensure the compatibility of security features with overall operations.

Changes in our Privacy Policy

Our Privacy Policy Statement may change from time to time. We will post any privacy policy changes on this page with an updated revision date. If there are significant changes in the Privacy Policy, we may notify you by other means, such as sending an email or posting a notice on our Agency website and/or social media pages prior to the effectivity of such changes.