Policy on Data Protection

This Data Protection Policy supplements the Code of Conduct and applies to all directors, syndics, employees, contractors, and third parties acting on behalf of Genneia or its controlled companies (all together, "**Genneia**" or the "**Company**"). Genneia requires its directors, syndics, employees, and third-parties acting on its behalf to follow this Policy to the fullest extent allowed by law.

Genneia is committed to respecting privacy rights, protecting Genneia's information, networks, systems and devices in its possession against cyber risks or attacks, maintaining transparency and ensuring appropriate use of collected information. The Company prioritizes responsibly collecting, handling, storing, processing and protecting personal information in compliance with applicable laws and regulations.

Policy Statement on Data Protection. Genneia will not tolerate violations of applicable data protection or privacy laws or noncompliance with Company policy. All directors, syndics and employees have a duty to keep non-public business information confidential and to protect collected personal information. Genneia requires that all information in its possession be stored securely and used only for legitimate purposes. Violations of Genneia's Data Protection Policy may result in corporate disciplinary action or sanctions. The Company expects that all third-party agents, suppliers, and customers with which it conducts business will comply with applicable data protection and data privacy laws.

Limitations on Use, Storage and Processing of Collected Data. Genneia may collect personal information and Personal Sensitive Information (PSI) as permitted by applicable law and according to this Policy. The Company may transfer personal information, including PSI, globally and to third parties for a legitimate purpose as consistent with applicable law. Genneia will retain personal information for no longer than necessary and will dispose of it in a manner that prevents loss, theft, misuse, or unauthorized access.

Limitations on Personal Sensitive Information: The Company reasonably limits access to Genneia information, including PSI, to authorized individuals who require access to the information for legitimate business purposes, including for employment matters and tax purposes.

Cyber Security and Data Protection. In connection with its Data Protection Policy and Integrated Management System Policy, Genneia seeks to secure its network systems and devices and all Genneia information. The Company relies on various cyber defenses to protect its network systems from attack, including firewalls and antivirus software. Genneia requires secure, password protected login access, obligates employees to change their passwords periodically, and maintains other appropriate access controls. Likewise, Genneia only grant access to the networks and network services to employees and third-parties acting on its behalf, who have been specifically authorized.

Records and Information Management. Genneia takes appropriate measures to retain business records and Genneia information in compliance with applicable laws. The Company periodically backs up corporate emails and documents stored on the server. Emails and documents are stored for the period defined in its procedures according to their classification. All financial records are retained for five (5) years and legal and tax records are retained for ten (10) years in accordance with applicable Argentine laws. The IT Department keeps a log of all data protection and data privacy incident reports for a minimum term of five (5) years, along with records of investigations into incident reports and the final decision.

This Q&A section answers common questions about the Data Protection Policy.

What is personal information? Personal information is any information relating to an identifiable person, such as a person's name, address, email, phone number, date of birth, or national identifier

that can be used by itself or in connection with other information to identify, contact, or locate a specific person.

What is personal sensitive information? Personal sensitive information (also known as "**PSI**") is any personal information that is non-public, confidential or otherwise sensitive in nature. PSI can include: financial information, such as a bank account or credit card numbers; patient health or medical data; personal data regarding children; and social security numbers or other personal identifying numbers.

What can I do to help protect Genneia from cyber risks? Genneia relies on you to take measures to mitigate cyber risks, such as data breaches, and fully protect Genneia information:

Prevent Unauthorized Access and Do Not Share Genneia Information:

- Limit access to Genneia information to authorized individuals for legitimate business purposes;
- Use strong passwords and change your passwords periodically, according to Genneia procedures;
- Ensure the most up-to-date security software is installed on your devices;
- Use Genneia-approved or provided devices, hardware and software for all business- related matters;
- Do not email Genneia information to your personal email or store or save Genneia information to unapproved devices, such as USB drives;
- Secure physical, hard-copy files, offices and information storage areas;
- Avoid and report phishing emails, social engineering schemes, or other attempts to improperly obtain Genneia information; and
- Do not disclose personal information, confidential or sensitive business information, trade secrets, or other non-public information related to Genneia or its employees.

You can monitor for cyber security threats and vulnerabilities and immediately report any cyber incidents, suspected breaches or concerns. You can also increase awareness about cyber security issues by advising third parties, suppliers, and customers to report any potential cyber vulnerabilities or concerns.

What incidents should be reported? Employees can report any suspected cyber security or data privacy incident, violation of law or Genneia policy according to the Compliance Reporting Policy.

How should I report suspected violations? Any person can report a suspected cyber incident or violation to Genneia. *You can make an anonymous report through the Compliance Reporting Form on Genneia's website at:* www.Genneia.com.ar under *Contact Us* or by emailing conducta.empresarial@genneia.com.ar. If you identify yourself, though, the Company can follow up with you to ensure that your concern is resolved and to provide feedback.

If you are an employee, all suspected data protection violations should be reported to your supervisor, the IT Department or IT Help Desk, or Human Capital. You can also make a report with Internal Audit, or the Chief Compliance Officer or email a written report to: conducta.empresarial@genneia.com.ar. All reports related to privacy or data protection complaints or incidents will be investigated and addressed according to the Compliance Reporting Policy and related compliance and IT procedures.