Artificial Intelligence (AI) Acceptable Use Policy

EnerSys, and its subsidiaries worldwide (collectively, "**EnerSys**", "**Company**", "**we**" or "**us**") recognize that the use of generative artificial intelligence tools like ChatGPT ("**AI Tools**") can increase employee productivity and innovation. EnerSys also recognizes that irresponsible use of AI Tools can pose risks to our operations and customers.

The purpose of this Artificial Intelligence (AI) Acceptable Use Policy (this "**Policy**") is to set forth the terms governing your access to AI Tools and provide guidelines for the responsible use of AI Tools while protecting the Company and mitigating the risks of misuse, unethical outcomes, potential biases, inaccuracy, information security breaches, and data exfiltration.

Access to and use of AI Tools is subject to this Policy and the Company reserves the right to amend, alter, or modify this Policy, or revoke access at any time.

Scope of Policy

This Policy applies to all EnerSys employees globally in the course of their employment and to any contractors or consultants accessing the Company's IT network or using Company owned equipment.

This Policy applies to all generative AI Tools, including AI-capable add-on technology available as part of third-party software already in use and approved by the IT Department. The list of pre-approved tools and applicable approval requirements can be found on the IT Department's Base Camp (SharePoint Online) page.

Principles for the Use of the AI Tools

EnerSys employees should observe the following principles when using AI Tools:

1. **Compliance with Legal and Regulatory Requirements**. EnerSys employees must comply with all applicable laws and regulations governing the use of AI Tools. This includes compliance with data protection and privacy laws, intellectual property laws, and anti-discrimination laws. At this time, certain countries have prohibited the use of certain AI Tools.
2. **Protection of Confidentiality and Corporate Property**. All software, hardware, systems, data files, information or data created, shall remain the property of EnerSys. Employees must ensure that they protect data and Company property when using AI Tools. The use of AI Tools must comply with the Company's Code of Business Conduct and Ethics.
3. **Compliance with Applicable Agreements**. Customers, including Government agencies, may have contractual restrictions on the use of open-source software, or may require specific notifications and restrictions on the use of AI Tools within the products and services they buy from EnerSys.
4. **Human Verification**. EnerSys employees must carefully review AI-generated material for inaccurate or incomplete information and potential infringement of third-party rights. You are ultimately responsible for all content produced with the assistance of AI Tools, as if you were the original creator. The source of AI-generated material should be disclosed when appropriate. AI automated decision-making processes are NOT acceptable practice.
5. **Cybersecurity**. Generative AI has the potential to increase the sophistication of cybersecurity attacks and compromise networks by helping scammers ingest as much information as possible about a target for purposes of manipulation, social engineering, and heightening the risk that malware, viruses, backdoors, or similar cybersecurity vulnerabilities are introduced into the Company's networks, software, products or services.

Please contact the Legal Department for further information or questions about these principles.

Prohibited Uses

Employees are prohibited from using AI Tools:

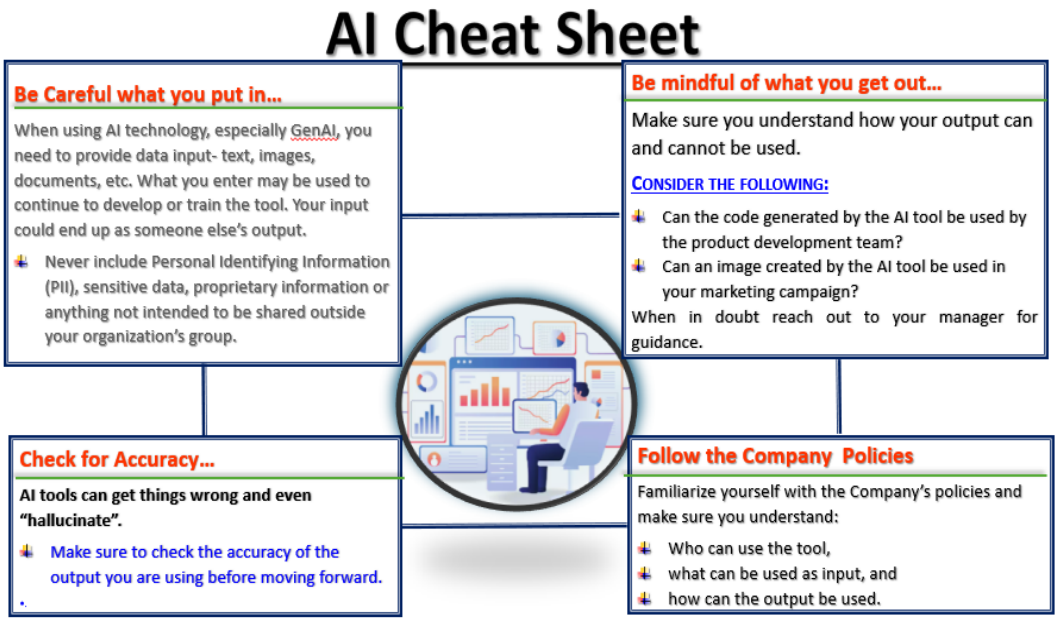
- in any way that violates any applicable federal, state, local, or international law or regulation (including, without limitation, any laws regarding the export of data or software to and from the US or other countries);
- to send, knowingly receive, upload, download, use, or re-use any material which violates the rights of any individual or entity established in any jurisdiction, including but not limited to data privacy rights and intellectual property rights;
- generate, edit, or verify documents containing highly sensitive information, special categories of personal data, or any other highly confidential information not intended to be in the public domain;
- interfere with the performance of their jobs, or of other employee's jobs, or engage in any other conduct that restricts or inhibits anyone's use or access to AI Tools, or which, as determined by us, may harm the Company or expose us to liability; and
- violate, attempt to violate, or knowingly facilitate the violation of the security or integrity of the Company's IT network, its software, products or services.

The Company has an enterprise subscription to certain AI Tools that allows for a more secure, private, and encrypted environment which is protected from the public open-source model. It may be permissible to use approved enterprise AI Tools to generate, edit, or verify documents, presentations, or materials containing confidential or proprietary information, in accordance with the other provisions of this Policy.

Required Actions to Request Access to Applicable AI Tools

To request access to applicable AI Tools requiring approval, please submit a request to IT via the request form link found on the IT Department's page on Base Camp (SharePoint Online). At a minimum you should expect to be able to explain the project or business purpose, confirm your acknowledgement of this Policy and associated training, and provide the approval from your direct Manager. The IT Department, and the Legal Department when required, will review and approve such requests on a case-by-case basis.

Acceptable Use and Content Standards



Note: AI "hallucinations" are misleading results or fictitious data that AI models generate which can be caused by insufficient training data, incorrect assumptions made by the model, or biases in the data used to train the model, among others.

If you are approved to use AI Tools, you should do so only for authorized, Company-related activities. You must use accounts created with EnerSys email addresses and credentials. In addition, your usage must comply with this Policy, EnerSys' Code of Business Conduct and Ethics, EnerSys data privacy and IT security policies, and the confidentiality obligations in employment documentation signed by EnerSys employees at the time of hire. Furthermore, you agree not to use AI Tools to knowingly upload, download, use, or re-use any material which:

- is copyrighted, involves trade secrets or know-how, is confidential, highly confidential, restricted, or used without adequate permission;
- is defamatory, obscene, indecent, abusive, offensive, harassing, violent, hateful, inflammatory, or otherwise objectionable;
- infringes any patent, trademark, trade secret, copyright, or other intellectual property or other rights of any other person;
- promotes any illegal activity, or advocates, promotes, or assists any unlawful act;
- deceives any person, impersonates any person, or misrepresents your identity affiliation or otherwise gives a false impression; or
- violates the legal rights (including the rights of publicity and privacy) of others or contains any material that could give rise to any civil or criminal liability under applicable laws or regulations.

You may only use vendor integrations or products featuring AI Tools that have been approved by the IT and Legal Departments. You should thoroughly review all AI Tool outputs before using them or forwarding them to others inside or outside the Company to:

- ensure that they do not contain biased, offensive, or discriminatory content;
- ensure that they do not contain cybersecurity vulnerabilities;
- ensure they do not improperly use or disclose personal or confidential information; and
- verify accuracy of reported facts with other trusted sources, especially when using large language models (LLM)-based AI Tools like ChatGPT.

If AI Tools are used for product development related activities, any code generated by such tools must be thoroughly verified and approved before integration into a product.

Monitoring and Enforcement

The Company, in its sole discretion, will determine whether your conduct is in compliance with this Policy. We have the right to:

- Monitor your use of AI Tools for any purpose in our sole discretion and as we see fit.
- Take any action we deem necessary or appropriate if we believe conduct violates this Policy, infringes any intellectual property right or other right of any person or entity, or creates potential liability for the Company.
- Take appropriate legal action for any suspected illegal or unauthorized use of property.
- Terminate or suspend your access to all or part of the AI Tools for any or no reason, including without limitation, any violation of this Policy.

Without limiting the foregoing, employees should be aware that EnerSys has the right to fully cooperate with any law enforcement authorities or court order requesting or directing us to disclose the identity or other information of anyone who accesses or uses AI Tools. In addition, EnerSys may conduct internal investigations or use a third party to investigate claims and allegations related to this Policy and your conduct.

Incident Reporting

As AI systems become more complex and autonomous, it becomes increasingly difficult for human operators to understand the underlying decision-making processes and intervene in time to prevent harm.

For this reason, it is important that users of AI tools and their managers conduct regular risk assessments to identify potential harms associated with AI systems. If while conducting these audits it is discovered that there has been a violation of this Policy or any of EnerSys' Policies, especially with regards to data privacy, cybersecurity, unintended disclosure of trade secrets, or there is potential harm to employees or customers, a report must be filed immediately with the Legal Department (legal@enersys.com) or the IT Department (it_help@enersys.com). The Chief Information Officer along with the Chief Legal & Compliance Officer shall determine whether a violation of this Policy has occurred and will consult with the relevant executives to determine corrective actions to be taken. Internal Audit shall report the results of any inquiry or investigation and the disposition of the matter to the Legal & Chief Compliance Officer. Depending on the conduct giving rise to the violation of EnerSys policies, inclusive of this Policy, disciplinary action, including termination of employment may be assessed.

Training and Recordkeeping

One or more virtual training courses will be available on the Company's learning management system (LiNK). In addition, general information, questions, or concerns with the use of any AI Tools may be directed to the Legal Department (legal@enersys.com) or the IT Department (it_help@enersys.com). Both departments will be responsible for keeping adequate records to evidence the employees who have received approval and the projects that were approved.

Other Policy and Use Guidance References

This Policy does not override other policies, procedures or internal controls for the Company. Any responsible use of AI Tools must comply with all relevant policies, internal controls, and guidelines of the Company, including those procedures and forms specific to the nature of the activity.

Please use the hyperlinks to access the other policies and use guidance referenced or incorporated herein:

- EnerSys Code of Conduct and Business Ethics
- Information Systems Acceptable Use Policy
- Global Information Security Policy
- Corporate Disclosure Policy
- Best Practices Guidance for the Ethical Use of AI in the Workplace
- Sensitive Personal Information Security Policy
- Applicable Privacy Policies (Americas, California, Europe, Brazil, Mexico, Australia, China and Singapore)