EasyGanttCharts Security Policy

Last Modified: May 17, 2023

Your privacy is important to EasyGanttCharts. Our only purpose in collecting and using your Personal Data is to provide you and your employer with Employee HR Management, Leave Management, TimeSheet Management, workforce scheduling, and other associated services.

Who We Are:

The product is owned by ProjectToolBelt LLC, a Wyoming-based company. Email customer service: support@EasyGanttCharts.com

We are committed to holding your data safe and secure. EasyGanttCharts's services are built around privacy and reliability, and we use trusted cloud providers to keep your data safe.

Product

We stretch beyond our abilities to ensure that our products and services are free of security flaws. In addition, we support the following security features to help keep your data safe:

- **Encryption:** Transport Level Security (TLS) is used to secure all data in transit, and all API and client communications (web and mobile) require HTTPS connections. All customer data, including email addresses, passwords, API keys, and third-party integration keys, is encrypted at rest.
- **Authentication:** All EasyGanttCharts workspaces support 2FA access and SSO via Google Apps. Teams, Business, and Unlimited workspaces can also enforce 2FA or use SAML authentication to manage access to their workspace.
- **Email Domain and IP Restrictions**: Customers on the Teams, Business, and Unlimited plans can limit access to their workspace to specific IP addresses or email domains.
- **Permanent deletion:** Users with the appropriate permissions can delete data associated with their account and workspace.

Infrastructure and Operations Procedures

The backend of EasyGanttCharts is hosted and managed within Amazon's secure data centres and uses Amazon Web Service (AWS) technology. Amazon performs ongoing risk management and submits itself to recurring audits to guarantee that it complies with industry standards.

For more information on AWS security, please visit https://aws.amazon.com/security/.

- **Hosting and Storing Data** The services and data of EasyGanttCharts are hosted in the United States.
- **Backups:** We perform full backups every 12 hours and log backups every 5 minutes, allowing us to restore the database as swiftly as possible in the event of a disaster.
- **Vulnerability scanning:** As part of our continuous delivery process, we perform manual vulnerability scans.

Reliability

To achieve 99.9% uptime across all of our products, our monitoring and logging systems are hosted separately from our production environment to guarantee uninterrupted reporting in the event of a system outage.

Security Measures

EasyGanttCharts's software development practices adhere to OWASP guidelines, protecting against common attacks.

- **Immutable infrastructure:** We do not modify live code or production servers. We treat our infrastructure as code whenever possible, and changes are tested and deployed automatically.
- **Continuous delivery:** We build, test, and release code multiple times a day using continuous integration and automated deployments.
- **Incident Response:** We have monitoring tools to escalate immediately and notify the team of security or availability incidents. These are hosted independently and not in our production systems.
- **Access to sensitive customer data:** Only a small group on our team can access sensitive customer data. If the team needs to access sensitive customer data, we will only do so after receiving written authorization from the customer via email.

EasyGanttCharts TECHNICAL AND ORGANIZATIONAL SECURITY MEASURES

EasyGanttCharts has implemented and maintains the controls listed here in accordance with industry standards generally accepted by information security professionals, such as Microsoft Security Hardening Guides, the OWASP Guide to Building Secure Web Applications, and various other Center for Internet Security Standards, among others, as necessary to reasonably protect Personal Data during storage, processing, and transmission.

- Assign responsibility for developing, implementing, and managing a comprehensive written information security program for the organization to an individual or a bunch of individuals.

- The relevant personnel must be adequately trained, qualified, and experienced to fulfill these functions and any other duties that might reasonably be expected to be carried out by the personnel responsible for safeguarding Personal Data.
- Create, maintain, and document reasonable technological, physical, administrative, and procedural safeguards, including, but not limited to, policies, guidelines, procedures, practices, standards, and controls that: - Ensure privacy, confidentiality, security, integrity, and availability of Personal Data; - Protect against any anticipated threats or hazards to the security and integrity of Personal Data; - Protect against any Security Incident.
- Regularly test, monitor, and evaluate the sufficiency and effectiveness of the information security program, including Security Incident response procedures.

Risk Assessment

- Conduct information security risk assessments at least once a year and whenever a material change in the organization's Business or technology practices may impact the privacy, confidentiality, security, integrity, or availability of Personal Data.

The risk assessment should include:

- Identifying and evaluating reasonably foreseeable threats, both internal and external, and associated risks to the privacy, security, confidentiality, integrity, and availability of Personal Data.
- Assessing the likelihood of and potential damage caused by identified threats and risks.
- Assessing the adequacy of personnel training concerning and compliance with the organization's information security program.
- Determining whether service provider agreements are adequate.
- Modifying and updating the organization's information systems and information security program to be adept and address material changes in relevant technology and business practices, personal data practices, and the sensitivity of personal data the organization processes and limiting and mitigating identified threats and risks.
- Keeping track of the risk assessment.
- Risk assessments should be conducted by third parties or any internal personnel not involved in developing or maintaining the organization's information systems or information security program.

Data collection, storage, and disposal

- Gather only the exact amount of Personal Data as is required to accomplish the purpose for which the information is collected;
- Avoid storing Personal Data on media connected to external networks unless necessary for business purposes;
- Prohibit the download and use of file sharing and other software that can pose security threats and vulnerabilities to areas or systems that hold Personal Data; and

- Securely dispose of personal data records so the information cannot be read or accessed.
- To prevent reusing any media that previously held sensitive information, it is imperative that you safely destroy that information.

Periodic Verification of Data Inventory

- Track and periodically inventory Personal Data collected, used, maintained, disclosed, disposed of, or otherwise processed by the organization, as well as the purposes for Processing such Personal Data.
- Conduct a periodic inventory check of the organization's information systems and assets that contain Personal Data.

Background Checks on Employees

- Conduct reasonable background verification checks (including criminal background checks) on any personnel or associated third parties who may have access to Personal Data or relevant information systems, and repeat the reviews at appropriate and adequate intervals.
- Maintain a policy that prevents individuals convicted of dishonesty, breach of trust, or money laundering from accessing Personal Data.

Personnel Education and Training

- Conduct training about the organization's information security program regularly and periodically for that personnel, subcontractors, and any third parties who hold access to Personal Data or relevant information systems
- Instill the importance of Personal Data security, confidentiality, and privacy; and the risks to the organization and its customers associated with Security Incidents.

Oversight and Management of Processors

- Take mindful steps and exercise due diligence while selecting and retaining subcontractors capable of ensuring and maintaining the confidentiality, privacy, security, integrity, or availability of Personal Data in alignment with the organization's contractual and other legal requirements.
- Hold subcontractors to deliver utmost responsibility by contractually demanding to maintain adequate and appropriate safeguards for Personal Data that are as equivalent to the safety standards that the organization must implement in accordance with contractual obligations; privacy

- Assess and monitor subcontractors on a regular basis to ensure they are in compliance with the applicable privacy and information security requirements.

Duties Separation

- Organizational personnel's duties and areas of responsibility should be separated to reduce the possibility of misuse of Personal Data or unauthorized or unintentional modification of the organization's information systems., Controls of Access.
- Identity personnel, classes of personnel, and third parties whose documented business functions and responsibilities necessitate access and permissions to Personal Data, relevant information systems, and the organization's premises.
- Grant authorized personnel, and third parties access to Personal Data, relevant information systems, and the organization's premises.
- Maintain an up-to-date record of personnel and third parties authorized to access Personal Data, relevant information systems, and the organization's premises.
- Establish user authentication protocols, secure access control methods, and firewall protection.
- Prevent terminated individuals, subcontractors, or other third parties from accessing Personal Data and information systems by removing their physical and electronic access to Personal Data and relevant information systems as soon as possible.
- User Authentication that is Secure Access to Personal Data and relevant information systems must be managed as follows:
  • Maintain secure control over login credentials, user IDs, passwords, and other authentication Identifiers. Establish passwords controlling access to Personal Data to have minimum complexity requirements and be at least eight characters in length.
  • Put in place a secure method for selecting and assigning passwords and use multifactor authentication and other reasonable authentication technologies.
  • Assign unique user ids and passwords that are not the Processor's default passwords.
  • Ensure personnel, subcontractors, and other third parties change passwords regularly based on the number of access attempts and whenever there is any indication of possible system or password compromise.
  • Change passwords frequently (at least every 90 days) for accounts that have access to Personal Data.
  • Do not reuse or recycle old passwords.
  • Only active users and accounts should access Personal Data and Block user access after multiple failed attempts to log in or access Personal Data or relevant information systems.
  • Restrict user access after a set period of inactivity.
  • Restrict or change access as soon as possible in response to personnel termination or changes in job functions.

Detection and Response to Incidents

Establish strict policies and procedures to detect, monitor, document, and respond to actual or reasonably suspected Security Incidents and to encourage reporting of such incidents, including

- Training personnel having access to Personal Data to recognize actual or potential threats and Security Incidents and to escalate and notify the senior management of such incidents.
- Mandatory post drawing attention to the -Security Incident review of events and actions taken concerning the security of Personal Data; Encryption: Encrypt personal data using industry-standard algorithms and key lengths.
- Stored on laptops, portable storage devices, mobile devices, or removable archival media.
- Stored in application databases or file servers.
- Stored outside of the organization's physical controls.
- Transmitted across any public network via wireless connections (such as the Internet).
- Transmitted through email attachments.
- During transit outside of the organization's information systems.
- Maintain policies that prohibit such storage or transmission unless necessary encryption is used.

Network Safety

Implement network security controls such as current firewalls, layered DMZs, and updated intrusion detection/prevention systems that include firewalls between the organization's information systems, the Internet (including internal networks connected to the Internet), other public networks, and internal networks not required for processing of the Personal Data; the firewalls must be sensibly designed to maintain the security of Personal Data and relevant information.

Data Separation

Physical or logical separation of Personal Data to ensure that it is not mixed with the information of another party unless approved by the Controller.

Detection of Malicious Code

- Implement and maintain software that detects, removes, prevents, and remediates malicious code designed to perform an unauthorized function on, or allow unauthorized access to, any information system, including, but not limited to, Trojan horses, computer viruses, worms, and logic or time bombs.
- Run malicious code detection software at least on a daily basis.
- Update malicious code detection software mandatorily every day, including by obtaining and implementing the most recent available versions.

Patch and Vulnerability Management

Maintain vulnerability management and regular patching procedures and technologies to identify, assess, mitigate, and protect against new and existing security vulnerabilities and threats, such as viruses, bots, and other malicious code.

Application Safety

Maintain application security and software development controls to prevent the introduction of security flaws into software developed by a Processor that processes personal data.

Change Controls

- Before implementing changes to the organization's information systems, use a documented change management process to assess the potential impact of such changes on the security, privacy, confidentiality, integrity, and availability of Personal Data, and ascertain whether such changes are consistent with the organization's information security program.
- No changes to the organization's information systems or information security programme should be made that increase the risk of a Security Incident or violate the organization's contractual or other legal obligations.

Off-Premise Information Security

- Maintain policies governing the security of records or media containing Personal Data stored, accessed, transported, and destroyed outside of the organization's premises.
- Track and document movement of records or media containing Personal Data; and
- Create copies of Personal Data before moving records or media containing the information.

Physical Safety

- Maintain reasonable restrictions utmost possible on physical access to Personal Data and relevant information systems (for instance., clean desk policy).
- Establish physical protection measures against damage from flood, fire, explosion, earthquake, civil unrest, and any other forms of natural or man-made disaster.
- Secure workstations with access to Personal Data when unattended by blocking physical access.
- Document all repairs and modifications to information security-related physical components of the organization's information systems.

Secure Disposal

Before sending any unencrypted hard disc, portable storage device, or backup media containing Personal Data offsite for maintenance or disposal, use secure destruction procedures to sanitize it.

Planning for the Unexpected

Establish and maintain policies, procedures, and guidelines for responding to a contingency or other occurrence that could jeopardize the security, privacy, confidentiality, integrity, or availability of Personal Data or harm the organization's information systems; such policies and procedures should include provisions for

- Creating and maintaining retrievable copies of Personal Data.
- Restoring any loss of Personal Data.
- Allowing the continuation of critical business processes involving Personal Data in emergencies.
- Assessing the criticality of specific applications and Personal Data in support of other contingency plan aspects.
- Periodic testing and revamping of contingency plans.