entigrity

ENTIGRITY PRIVATE LIMITED &
ENTIGRITY SOLUTIONS LLC
IT & CONFIDENTIALITY POLICY

UPDATED Jan ‘20

DISCLAIMER:

Entigrity Solutions LLC (*herein referred to as* Entigrity *in this document*) is committed to ensuring the Confidentiality, Integrity, and Availability (CIA) and provide comprehensive protection to its information assets against the consequences of confidentiality breaches, failures of integrity and/ or interruptions to their availability.

This document details Entigrity policies to ensure the protection of its information assets, and to allow the use, access, and disclosure of such information in accordance with appropriate standards, laws, and regulations. All employees (team members), customers, and third parties who use Entigrity's information processing facilities are required to comply with the Information Security policy of Entigrity.

To provide adequate protection for information assets, Entigrity has built the Information Security Management System (ISMS) and certified and approved for ISO 27001:2013 standard which includes the respective policies to be followed in a diligent, consistent, and impartial manner. Entigrity will implement procedures and controls at all levels to protect the confidentiality and integrity of information stored and processed on its systems and ensure that information is available only to authorized persons as and when required.

All the existing Entigrity policies, relating to personnel, administration, protection of confidential information, computer systems, network infrastructure, data storage and other areas would apply equally to the information systems environment. The Information Security policies apply to any person (directors, employees, consultants, clients and third parties), who accesses and uses Entigrity information systems.

We would also like to mention that we always strive to mitigate every risk to client data by building a robust working environment that operates smoothly and protect the shared information from malware, ransom ware, data theft, phishing or any such threat. However, in the era of advanced Information Technology, no system is deemed 100% fool proof and carries certain vulnerabilities.

OBJECTIVE

Continual improvement in the effectiveness of Information Security Management System (ISMS) at Entigrity is demonstrated through the use of Security Policy, Security Objective, Audit Results, Analysis of Data, Corrective and Preventive Actions, and Management Review. These safeguards have been designed to:

- ✓ Ensure the security and confidentiality of client information,
- ✓ Protect against any anticipated threats or hazards to the security or integrity of such information
- ✓ Protect against unauthorized access to or use of client information that could result in substantial harm or inconvenience to any client.

In addition to these risks, other specific areas of risk for consideration for in this policy are:

- ✓ Unauthorized access and/or use of personal client information by means of computer and electronic data, or paper documents and files
- ✓ Unauthorized access and/or use of personal client information by third party vendors, and
- ✓ Unauthorized access to the data processing or telephone communication system.

ISO 27001 CERTIFICATION

Entigrity is an ISO 27001:2013 certified company. In accordance to the guidelines mandated by ISO 27001:2013 standards, Entigrity has developed compliance and directives to establish appropriate conduct relating to the administrative, technical and physical safeguards of client records and information. Entigrity has established, implemented, maintained and continually improves the within the context of its overall business activities and risks it may face in accordance with the requirements of the ISO 27001:2013 standard.

The scope of the standard includes:

- ✓ Identifying and assessing the risks
- ✓ Implementing controls and procedures for incident handling
- ✓ Implementing training and awareness programs
- ✓ Monitoring the procedures and other controls
- ✓ Managing operations and resources
- ✓ Undertaking regular reviews of the effectiveness of ISMS
- ✓ Conducting internal ISMS audits
- ✓ Recording actions/events potentially impactful on the effectiveness or performance of ISMS
- ✓ Implementing and maintaining and improving the ISMS
- ✓ Ensuring that the improvements help achieve their intended objective.

Entigrity agrees to implement appropriate technical and organizational measures designed to protect Customer Personal Data, Employee and third-parties data, as required by the Applicable Data Protection Law(s). Further, Entigrity agrees to regularly test, assess, and evaluate the effectiveness of its Information Security Program to ensure the security of the Processing. Entigrity has comprehensive privacy and security assessments and certifications performed by regulatory or third parties. Such certifications include ISO 27001: 2013 certifications.

VIOLATION

Any team member found to have violated this policy may be subject to disciplinary and/or legal action as per company's and prevailing regulations.

COMPLIANCE AND PROCEDURES

Entigrity has established a formal policy and process for the requirements and key information security considerations for information technology operations, including the definition of standard operating procedures, change management, configuration management, release management, information backup, and restoration and cloud computing.

There are a number of controls in place to achieve the protection of data, information, and information system:

- **Access Control**
- **Logging and Monitoring**
- **Operational Control**
- **Information System Audit Control**
- **Password Management**

ACCESS CONTROL

- ✓ Access to data restricted on business' "need-to-know". - Access to customer information via the Entigrity's computer/network system is limited to those employees who have a business reason to know such information.
- ✓ All the work station and computer system are password protected. Also we follow strict password policy with strong random password approach.
- ✓ Administrative or Network access to network devices is logged and only available to authorized IT Personal.
- ✓ Access to electronically stored records containing personal information are electronically limited to those employees having an authorized and unique login ID assigned.

- ✓ Unique ID assigned to each person with system and cloud access to data. The ID and the access is revoked as soon as the association with Entigrity comes to an end.
- ✓ The files shared by the clients are allowed only to be worked upon from the work station either on cloud or through logging in remotely into client computer. We don't allow an upload or downloads of client files or data unless specifically approved by client in writing. Under no circumstances it is allowed to be stored on the hard drive of the computer.
- ✓ Printing, writing down information, taking pictures/snapshots of screen or transferring information to a third party through emails or by any other means is strictly prohibited.
- ✓ All the USB port/CD-ROM/ are disabled.
- ✓ Uploading or downloading of any kind of information, documents, videos, photos, spreadsheets, files, folders etc is strictly not allowed.
- ✓ No one is allowed to carry mobile phones, pagers, tablets, outside electronic or smart devices, memory storage device such as pen drives, memory cards or such articles to the operations areas. The valuables safely required to deposited and to be stored at the assigned lockers.
- ✓ We don't allow paper or printers or pen or any such thing in any of the core work areas were we perform our client operation or client related work. The place where client work is carried are partitioned properly and also segmented from other areas of the office.
- ✓ Each of our entry and exits whether in the within chamber or in office are key card enabled and controlled.
- ✓ We continuously monitor to improve our access security so access social media sites like facebook, youtube, Instagram etc or news portal or personal emails or financial portals or entertainment sites are strictly not allowed unless specifically permitted by the client in writing.
- ✓ We can also facilitate multi-factor authentication if that may be required by our client and can further restrict access to their computer system or data.

LOGGING AND MONITORING

- ✓ Every employee is provided with a unique access card as a part of ID badge. It is used to access the operations areas and mark the individual attendance at office and respective work areas. Each entries and exit are logged in the system to monitor the movement even the within the office premises.
- ✓ Provision of access card is strictly made on the basis of work and is limited to the areas where the employee works. Tailgating is strictly prohibited.
- ✓ Ad hoc security check of every employee is done during entry and exit from work areas.

- ✓ The whole premise, including the exterior and interiors are monitored under CCTV surveillance with 24x7. The footage is stored centrally to fetch the records if need be. We keep about 60 days records of the footage as required by the law.
- ✓ Personal computing devices, memory storage devices such as smartphones, ipads, tablets, etc. personal emails, suspicious websites and downloads allowed on Entigrity network/computers. IT admin must ensure to block social media, video streaming and personal email domains on all computers.
- ✓ Edibles are not allowed to be carried into the work areas. The employees are only allowed to carry drinking water bottles to be kept with them at their desks.
- ✓ Computers are not left unmanned, if need be, they have to be password locked with screen savers. Desks need to be kept clean at all times.
- ✓ If required, IT admin to sample emails from time to time for the type of data being exchanged and prohibit any unauthorized emails.
- ✓ Where practical, all visitors who are expected to access areas other than common space or are granted access to office space containing personal information should be required to sign in at a designated reception area where they will be assigned a visitor's ID or guest badge and escorted at all times. Visitors are required to wear said visitor ID in a plainly visible location on their body.
- ✓ Visitors cannot carry any external devices or electronic devices or wallet with them in the operations areas.
- ✓ All our computer work station and computer system are Quick Heal Secured which protect it from any malware or spyware or data theft or external attack also it restricts access via USB Drives/CD-ROM/External Drives.
- ✓ Monthly audit is done by Data Protection Officer and Internal Auditor on the process and any lapses minor or major are immediately report and corrective action are immediately taken.

OPERATIONAL CONTROL

- ✓ All computers with an Internet connection or any computer that stores or processes personal information must have a recently updated version of software providing virus, anti-spyware, and anti-malware protection, installed and active at all times.
- ✓ All the computers shall have licensed version of Windows, Microsoft Office, Skype Accounts, Office Email on Microsoft Outlook.
- ✓ All computers are to be USB disabled so that even if someone smuggles a portable memory device to the workstation it won't work. The network administrator gets a quick notification about any such attempt.
- ✓ The whole operational area has to be maintained paperless. No pens, pencils, or stationery to be allowed in these areas. Printers are not to be installed in these areas. 'Work from home' is strictly not allowed.

INFORMATION SYSTEM AUDIT CONTROL

- ✓ Install and maintain an effective network firewall to protect data accessible via the Internet.
- ✓ Enterprise level Quick Heal antivirus to be installed and regularly updated on all workstations, protecting against virus from internet, emails or any other domain.
- ✓ Operating system and application software security patches to be kept up-to-date.
- ✓ Use of only licensed software on all Entigrity computers or clouds. Periodic updates to all the software being used as and when available.
- ✓ Stored data to be encrypted and sent across open networks only after encryption.
- ✓ Wherever applicable, multi factor authentication to be used.
- ✓ The IT admin needs to ensure that there is no access to personal emails, social networking sites, video streaming platforms or applications, websites with potential malware.
- ✓ Downloading of exe files, or any other multimedia files unless required by the process and approved by the client has to be blocked by the IT admin.

PASSWORD MANAGEMENT

We have processes designed to enforce minimum password requirements for access to or through Entigrity Systems. We currently enforce the following requirements and security standards for end user passwords at Entigrity.

- ✓ Passwords must be a minimum of 8 characters in length and include a mix of uppercase and lowercase letters as well as numbers and symbols.
- ✓ Multiple sign-ins with the wrong username or password result in a locked account, which will be disabled for a period of time to help prevent a *brute-force sign-in*, but not long enough to prevent legitimate users from being unable to use the application.
- ✓ Email-based password reset links are sent only to a user's pre-registered email address with a temporary link.
- ✓ Entigrity prevents reuse of recently-used passwords.

All access to Entigrity systems and services are reviewed by IT Admin and updated on a weekly basis to assure proper authorizations are in place commensurate with job functions.

COMPLIANT WITH IRS TAX PAYER DATA SAFEGUARDS MEANT FOR BUSINESSES

As mandated by the IRS protecting taxpayer data is the law. Federal law gives the Federal Trade Commission authority to set data safeguard regulations for various entities, including professional tax return preparers. According to the FTC Safeguards Rule, tax return preparers must create and enact security plans to protect client data.

The recommendations outlined here are for all systems that receive, process store or transmit FTI, including Tumbleweed workstations and server, database servers, application servers, file servers, mainframes, routers, switches and firewalls. To read in detail about the recommendations and standards please click here:

1. Publication 1345 (Rev. 12-2019) - outlining our responsibility as an Electronic Return Originator, including in the area of e-File security and privacy.
2. Publication 4557 (Rev. 6-2018) - an overview of tax professionals' obligations to protect taxpayer information and provides a step-by-step checklist for how to create and maintain a security plan for our digital network and offices.
3. Small Business Information Security: the Fundamentals - To provide small businesses with an overview of those steps to security data. Its focus is on five principles: identify, protect, detect, respond and recover

Entigrity complies with the IRS standards and recommendations as mentioned in the aforementioned publications by the IRS.

NETWORK SECURITY

Entigrity has deployed an information technology network to facilitate its business and make it more efficient for various risks. And establish management direction, principles, and standard requirement to ensure that the appropriate protection of information on its networks maintained and sustained. Few controls which in place to achieve the protection of exchanged information from interception, copying, modification, misrouting, and destruction as follows:

- ✓ **Network Controls**: Entigrity monitors and updates its communication technologies periodically with the goal of providing network security as per industry best practices cryptographic techniques are used to protect the confidentiality, integrity, and authenticity of sensitive and confidential information. Firewall rules and access restrictions are reviewed for appropriateness on a regular basis.

- ✓ **Infrastructure Controls**: Entigrity uses an Intrusion Detection System (IDS), a Security Incident Event Management (SIEM) system and other security monitoring tools on the production servers hosting the Entigrity product service. Notifications from these tools are sent to the Entigrity Security Team so that they can take appropriate action.

- ✓ **Secure Communication**: All data transmissions to Entigrity services are encrypted using TLS protocols, and we use certificates issued by SHA 256 based CA ensuring that our users have a secure connection from their browsers to our service. We use the latest and updated cipher suites Entigrity Products are always communicated via HTTPS using Transport Layer Security (TLS), a cryptographic protocol that is designed to protect against eavesdropping, tampering, and message forgery.

Entigrity server is always connected to the web-app via HTTPS using Secure Sockets Layer (SSL), a cryptographic protocol that is designed to protect against eavesdropping, tampering and message forgery.

Retention and disposal guidelines for all business correspondence including messages, in accordance with the defined standard.

Segregation of the network shall be done by establishing V-LAN/ DMZ architecture. In either case, Testing, Production and Development environment shall be segregated as well.

Agreements have been established for the secure transfer of business information to external parties (such as customers, suppliers, and other interested parties).

The roles and responsibilities for management of network security shall be clearly defined, communicated and reviewed on a regular basis to ensure optimum operative effectiveness and necessary segregation of duties shall be done to attain the said objective.

COMMITMENT

Entigrity has established a formal Compliance Policy and Procedure which addresses aspects of compliance required to be adhered to and fulfilled with respect to Entigrity's Information Security Policies. This policy addresses the legal and compliance requirements pertaining to relevant statutory legislation and contractual & regulatory obligations which Entigrity is supposed to adhere to in order to protect its documents, records and assets, thereby preventing the misuse of information processing facilities. Such efforts would help Entigrity establish, maintain, and sustain the desired information security and privacy posture aligned with the Entigrity strategic business plan, based on the best practices, standards and principles.

Entigrity is committed to and conducts its business activities lawfully and in a manner that is consistent with its compliance obligations. The Legal and Regulatory Compliance (Compliance Policy) establishes the overarching principles and commitment to action for Entigrity with respect to achieving compliance by:

- ✓ Identifying a clear compliance framework within which Entigrity operates.
- ✓ Promoting a consistent, rigorous, and comprehensive approach to compliance throughout Entigrity.
- ✓ Developing and maintaining practices that facilitate and monitor compliance within Entigrity.
- ✓ Seeking to ensure standards of good corporate governance, ethics, and community expectations.
- ✓ Engendering a culture of compliance where every person within Entigrity accepts personal responsibility for compliance, and acts ethically and with integrity.

Entigrity has been identifying all relevant regulatory and legislative requirements as per its contractual requirements and organization's operational requirements and defining, documenting, and updating it on a regular basis.

All records, as mandated by statutory/legal/regulatory authorities in India or of foreign origin, for which Entigrity is responsible for compliance, will be protected from intentional or unintentional damage through natural causes.

The retention limit of statutory records will be as mandated by the applicable legislation. However, for business records/documents, the business heads and or Entigrity management shall determine the retention limit with justification.

Entigrity will always seek to protect the privacy of the personal information of its customers, employees, and third parties with whom Entigrity has signed the agreement. Divulging of facts will be done only in keeping with statutory /contractual/regulatory/legal requirements. Such information will always be protected from getting misused, leaked, or falsified or traded with any interested party knowingly or unknowingly.

Where logs are required to be maintained as per contractual/regulatory/statutory/legal requirements, these will be maintained for a specified duration.

Data or records that are no longer required for business, legal, and/or regulatory purpose will be disposed of securely.

As part of the information security audits by independent consultants or body, the appropriate confidentiality and non-disclosure agreements will be signed with them. And any access granted to the external shall be restricted immediately after completion of the audit.

REPORTING SECURITY AND PRIVACY BREACHES

Entigrity follows policies and procedures to detect, respond to, and otherwise address security incidents including procedures to:

- Identify and respond to suspected or known security incidents followed by mitigating their harmful effects and documenting these incidents along with their outcomes.
- Restore the availability or access to Customer Personnel.
- Retrieve data in a timely manner.

Entigrity has a Security Incident Response Plan designed to promptly and systematically respond to security, privacy, and availability incidents that may arise. The primary focus of the plan is detecting, analyzing, prioritizing, and handling security incidents. As an important component of Entigrity's Information Security Management program the incident response plan is tested and refined on a regular basis.

Notice: Entigrity agrees to provide a prompt written notice within the time frame required under Applicable Data Protection Law(s) to a customer's Designated POC if it knows or suspects that a security incident has taken place. Such notice will include all available details required under Applicable Data Protection Law(s) for the customer to comply with its own notification obligations to regulatory authorities or individuals affected by the security incident.

Typically we inform about the incident within the less than 1 hours to the appropriate stakeholders.

Under no circumstances should a user attempt to resolve any security and privacy breach on their own without first consulting the Entigrity management. Users may attempt to resolve security and privacy breaches only under the instruction of, and with the express permission of the DPO.

Business Contingency and Disaster Recovery

- Entigrity has established a formal business contingency management (BCM) plan and a Disaster Recovery Plan (DRP) to minimize downtime of the critical business process, and recovery within required and agreed business timescales in the event of a disaster. Entigrity has also created a clearly defined framework for the ongoing management of the BCM activities and provide guidelines for the development, testing, maintenance, and implementation of business continuity plans.

Entigrity defines two categories of systems from the disaster recovery perspective (DRP):

- **Critical Systems**: These systems host application servers and database servers or are required for the functioning of systems that host application servers and database servers. These systems, if unavailable, affect the availability of data and must be restored, or have a backup process to restore these, immediately on becoming unavailable.
- **Non-Critical Systems**: May affect the performance and overall security of critical systems, do not prevent critical systems from functioning and being accessed appropriately. These systems are restored at a lower priority than critical systems.

Backup: To prevent data loss due to human error, our application databases are backed up every hour in an automated fashion. A comprehensive check of the backup is carried out once every week to ensure the backup is error free and maintains data integrity.

Data Replication: Our customer and application databases are timely replicated on backup servers along with our CDN servers which are geo-redundant.

Location: We store customer data in a secure data center at an offsite location in the US.

Internet Redundancy: Entigrity is connected through multiple Tier-1 ISPs. So, if anyone fails or experiences a delay, you can still reliably get to your applications and information.

DRP is tested on a half-yearly basis; and the results are documented, and revisions are made, as necessary.

IMPLEMENTATION, TESTING AND ADJUSTMENTS

Entigrity reviews security reports to ensure that no attempt has been made by non-employees to gain access to the institution's computer information system. Also, system computer maintenance reports are reviewed to ascertain that no unauthorized changes have occurred to customer account information or personal data.

Inappropriate access to information could result in the filing of a Suspicious Activity Report (SAR), employee counseling, and/or termination. A SAR may also be filed if a non-employee, such as an outside intruder, or employee of a third party vendor, attempts unauthorized activity.

The Privacy Policy, Privacy Notice and Customer Information Security Policy are reviewed annually with all employees. Other training is provided to protect against destruction, loss, or damage of customer information due to potential environmental hazards, such as fire and water damage or technological failures. All of this training will help minimize risk and safeguard customer information security.

CONTRACT

All Entigrity contracts will clearly define each party’s data protection and information security responsibilities toward the other by detailing the parties to the contract, effective date, functions or services being provided (such as defined service levels), liabilities, limitations on use of subcontractors and other commercial/legal matters normal to any contract.

The processing must be governed by a contract in writing between the controller and the processor, setting out the following:

- Subject matter and duration of the processing
- Nature and purpose of the processing
- Type of personal data and categories of data subjects involved
- Obligations and rights of the controller and processor

Entigrity shall adhere to all its contractual responsibilities of confidentiality and privacy and shall take all appropriate measures and actions in order to implement and enforce highest standard of confidentiality and privacy towards it clients, contractors, or any other stakeholder.

DUE DILIGENCE

Entigrity performs due diligence in its review of its service providers for the protection of customer information. By contract, Entigrity requires that service providers have controls in place to ensure that they and any subcontractor used by the service provider will also be able to protect customer information. The institution requests copies of audits and test result information that indicate that the service provider implements information security measures. ISO reviews the information annually.

Before contracting with a third-party supplier, it is incumbent upon Entigrity to exercise due diligence in reaching as much understanding as possible of the information security approach and controls the company has in place. It is important that the documented “supplier due to diligence assessment" procedure is followed so that all the required information is collected and an informed assessment can be made.

References for new employees are checked. During orientation, each new employee will receive proper training regarding the institution’s Privacy and Customer Information Security policies and the importance of confidentiality. He or she is trained in the proper use of computer information, passwords, and codes. Training also includes controls and procedures to prevent employees from providing customer information to an unauthorized individual, including "pretext calling" and how to properly dispose of documents that contain personal identifying information.

GDPR COMPLIANCE

Pursuant to compliance under General Data Protection Rules (EU), board of Entigrity has allocated necessary resources for its compliance as well as implementation and fully understand its implications. Board of Entigrity hereby takes full responsibility of GDPR compliance.

Mukund Patel has been designated as Data Protection Officer (DPO) and can be contacted at mukund.patel@entigrity.com

As mandated by GDPR requirements, we have

- Mapped dataflow within the organization, identified the risks as well as assessed those risk areas and implemented corrective actions for the same.
- We have developed necessary operational policies and procedures to comply with the requirement.
- Ensured necessary staff training during the appointment and other ongoing training as necessary thereafter.

We also continually assess our internal audit and compliance. As and when required, we take necessary steps to improve the same.

VIOLATION

Entigrity Employee:

All Entigrity employees must hold any confidential information in trust and confidence, and not use or disclose it or any embodiment thereof, directly or indirectly, except as may be necessary in the performance of duties for the respective client or as otherwise required by law or contract.

Employees may not remove confidential information stored on local computers, servers or network, or duplicate confidential information, unless authorized by the employer to do so. Upon termination of any assignment or as directed by a supervisor, employees shall return all such materials and copies thereof to their proper location in the organization.

For the commission of any of the offenses that violate the IT privacy policy, an employee shall be subject to disciplinary action and legal action as may advised in law including but not limited to immediate termination of employment. Disciplinary action for the same or different offenses shall progress in the following manner:

Verbal warning. Verbal statement to employee that he/she has violated a rule and/or regulation and that such violation may not continue. If the violation is petty and non-repetitive.

Written reprimand. Formal notification in writing to employee that he/she has violated a rule and/or regulation. If violation is petty but repetitive.

Suspension / Termination / Legal Action. Loss of work and wages for a specific number of hours or days, depending on the severity of the offense. Notice of suspension is provided to the employee in writing. For serious violator or regular offenders or intruders etc.

ASSIGNMENT OF RESPONSIBILITY

Entigrity will be responsible for the development, implementation and maintenance of the security program and will assign specific responsibility for its implementation and administration. Management will review the standards set forth in this policy and recommend updates and revisions as necessary. It may be necessary from time to time to adjust the plan to reflect changes in technology, the sensitivity of customer data and internal or external threats to information security.