DATA PRIVACY AND SECURITY PLAN

Thrively is committed to ensuring data security and privacy in compliance with all relevant and prevailing laws, and in alignment with the NIST Cybersecurity Framework, which serves as the industry standard for data protection policies.

For every contract, Thrively follows a defined process that materially addresses security and privacy requirements, including adherence to NIST guidelines. This ensures that customer data and systems remain secure at all times.

Outlined below are the key sections of the NIST Cybersecurity Framework and the corresponding controls deployed by Bloom Software Inc., DBA Thrively, to ensure that customer data and privacy are never compromised.

PROCESS & OPERATIONAL CONTROLS		
1	Applicable data security and privacy contract requirements over the life of the Contract	* Security Access controls Based on Employee roles & Responsibilities * Data management processes by identifying and classifying Confidential, Public, Private data, Sensitive & Non-sensitive PII * Enabling encryption both for Data at rest and Data in transmit * Regular updates of Development and Administrative software * Employee Awareness program * Encrypted data backups * Choosing Secure Cloud Hosting platform by reviewing their security & privacy credentials, certifications, thereby ensuring third-party and vendor security
2	Administrative, operational, technical safeguards and practices that are in place to protect PII	* Security measures in place to ensure unauthorized access, remove, change or disclose PII by way of implementing encryption, firewalls, IPS, regular security Audit. * Conduct Annual internal Audit to identify Risks, Gaps and define Scope of Improvement. * Employee awareness programs are conducted on a regular basis.
3	Training received by our employees and subcontractors (If Any) engaged in the provision of services under the contract on the federal and state laws that govern the confidentiality of PII	* Internal Awareness program is conducted by ISO certified Cyber Security Management team. The program outlines the need to govern PII, security measures in place around the governance & ensure security responsibilities are adhered to by each individual employee. * Annual internal audits are performed to fix any gaps identified by reviewing evidence of each security process.

4	Contracting processes that ensure that our employees and subcontractors (If any) are bound by written agreement to the requirements of the Contract, at a minimum	Employees are bound by NDA and Confidentiality Agreement outlining the security expectations and the adherence guidelines during their employment.
5	Managing data security and privacy incidents that implicate PII and describe specific plans you place to identify breaches and/or unauthorized disclosures, and to meet your obligations to report incidents	* Measures in place – Encrypting sensitive data, Implementing data retention and disposal policies, Awareness program for employees on data security, Adopting anti-malware practices & by implementing end point protection, Implementing access management, Regular risk assessment is conducted, Regular encrypted data backups, Managing third-party risks, A Disaster recovery procedure in place to replace the affected device and ensure productivity is back to normal in minimal time, Periodic tabletop exercise is conducted to rehearse incident response process, Incident report in place describing the incident, measures taken to eliminate associated risk. * Reporting - An incident is identified and the affected device is isolated to limit the breach, The incident is reported to relevant Stake holders & Authorities (wherever applicable) through appropriate communication channel & Evidence is secured for forensic investigation purposes, Provide point of contact to relevant stake holders and authorities to ensure follow-up questions are responded appropriately and in time
6	Process of Data transitioned when no longer needed by us to meet contractual obligations	Will be provided via a secured file transfer method
7	Secure destruction practices	Third party enterprise tools are used to destruct data in a secure manner. The tool provides a report, which clearly outlines the relevant data is destroyed in a secured manner. The report will be published to relevant stakeholders on request.
8	Data Security and Privacy program/practices	Our program/practices are in line with the NIST framework/guidelines.

NIST FRAMEWORK CONTROLS		
CATEGORY	FRAMEWORK REQUIREMENT	CONTROLS IN PLACE
IDENTITY (ID)	Asset Management : The data, personnel, devices, systems, and facilities that enable the Organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	Thrively has a defined Asset Management policy which outlines how an asset is built, managed and maintained. * Devices are hardened by deploying end point controls, protection against data loss, malware, antivirus. Software relevant to respective projects are installed. Administrative rights are revoked, thus ensuring software isn't installed without proper approvals by authorities. * Network Access controls in place * Facility in manned by Security personnel and access to work area is allowed only to authorized personnel by an access card. Visitors have to report to security personnel and an entry in visitors' books has to be made. Visitors are allowed inside the work area with appropriate approvals from Employee whom the visitor wish to visit.
	Business Environment : The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	* Employees have restricted access to production environments * Roles and responsibilities are defined in the way of Induction and awareness programs. * Induction is carried out when an employee joins the organization. * Project specific roles and responsibilities are made explicit during onboarding to the respective Projects.
	Governance : The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	* Policies, guidelines are defined in a portal and all employees are mandated to read and understand the policies. An annual security awareness program has to be viewed and accepted. * The policies, guidelines are reviewed annually and any changes/updates incorporated. * These policies are approved by the management and uploaded to the portal. Post the new policy deployment, all employees are mandated again to read, understand and adhere to the policy, guidelines.
	Risk Assessment : The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	Controls, policies, and processes are implemented in line with NIST framework. The controls, processes are reviewed annually on a time-to-time basis and changes incorporated as necessary. Processes are broadcasted as part of induction or awareness programs.

	Risk Management Strategy : The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	A periodic risk review is conducted and a risk review meeting is carried with the executive management. Post the review meeting, risks are treated appropriately and mitigated.
	Supply Chain Risk Management : The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.	A risk review process is in place by reviewing vendors risk assessment process wherever applicable

PROTECT (PR)	Identity Management, Authentication and Access Control : Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of authorized access to authorized activities and transactions.	Yes. Role based access provided to physical, logical assets. Physical assets like facility have access to employees only. Visitors, on a need basis only, are always escorted by the security personnel or relevant authority. Logical assets like source code repository have role-based access i.e. read only access, write access and administrative access. These accesses are periodically reviewed and necessary changes made as per organization/project requirements.
	Awareness and Training : The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.	Yes, as part of corporate induction and project onboarding induction. Additionally, all employees are mandated to take a security awareness session by going through a video. Employees are also mandated to read, understand policies, guidelines and adhere to them.
	Data Security : Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	By providing role-based access. The access is provided with relevant approval by the project manager and they are reviewed periodically
	Information Protection Processes and Procedures : Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage	Corporate Information security policy, Information classification policy and information policy risk management defined.

	protection of information systems and assets.	
	Maintenance : Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	Annual maintenance contracts in place.
	Protective Technology : Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	Devices are hardened, end point controls implemented and role-based access provided

DETECT (DE)	Anomalies and Events : Anomalous activity is detected and the potential impact of events is understood.	Periodic vulnerability assessments and penetration testing carried. Detected anomalies are fixed in a timely manner. Firewall deployed and end points are periodically updated with Operating systems, Development software patches
	Security Continuous Monitoring : The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	Intrusion prevention system in place. User system is deployed with end point controls. Devices are regularly updated with relevant Operating system and development software patches. End of support devices are replaced with appropriate devices and in a timely manner.
	Detection Processes : Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	Periodic vulnerability assessment and penetration testing are carried out.

RESPOND (RS)	Response Planning : Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.	Incident response policy in place
	Communications : Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).	Yes.
	Analysis : Analysis is conducted to ensure effective response and support recovery activities.	Periodic vulnerability analysis and penetration testing carried out.
	Mitigation : Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	The affected device is isolated and replaced by a recovery device to ensure business continuity. Affected devices are analysed, issues fixed and restored in a timely manner.
	Improvements : Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	All the issues are recorded in the Incident response report and incorporated as lessons learnt. These incidents are also reviewed during risk management review meetings and the effectiveness of lessons learnt are measured.

RECOVER (RC)	Recovery Planning : Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.	Annual disaster recovery exercise is carried out in line with Business continuity and Disaster recovery plans.
	Improvements : Recovery planning and processes are improved by incorporating lessons learned into future activities.	Yes & reviewed during Audits & Review meetings
	Communications : Restoration activities are coordinated with internal and where ever applicable external parties	Yes