Dynatron

DYNATRON SOFTWARE INFORMATION SECURITY PROGRAM

Dynatron

VERSION CONTROL

Version	Date	Description of Changes	Updates Completed by:	Approval
1.0	7/13/2020	Document Creation	Program Management	Cyber Committee
1.0.1	7/20/2020	General edits and revisions	Program Management	Cyber Committee
1.0.2	8/10/2020	General edits and revisions	Program Management	Cyber Committee
1.1	8/3/2022	Updated for current Cyber Program and process inclusion	Program Management	Cyber Committee
2.0	3/24/2025	Document updated for current reflection of Cyber Program and Leadership, as well as process updates and inclusions.	Cyber Staff	Senior Cyber Program Leadership
2.1	2/24/2026	Annual Review Updates reflecting current state of organization.	Marie Weeks	Matt Uptain
2.2	6/26/2026	Branding and content updates to reflect current state.	Cyber Staff	Matt Uptain

Dynatron

I. Overview

Dynatron Software's business operations require the protection of information assets to preserve confidentiality, integrity, availability, and processing integrity of data entrusted to the organization.

This Information Security Program establishes the governance framework, policies, standards, and controls necessary to safeguard Dynatron Software and customer information, mitigate cybersecurity risks, support operational resilience, comply with applicable legal, regulatory and contractual requirements, and provide oversight and accountability for information security activities.

The program aligns with recognized cybersecurity frameworks and industry best practices and is reviewed at least annually.

Dynatron Software achieved SOC 2 Type 1 attestation in 2026, affirming that our security controls are suitably designed. We are currently building the evidence window required for SOC 2 Type 2 attestation.

Dynatron Software's Information Security Program is risk-based and aligned with recognized cybersecurity frameworks and industry best practices. The Program incorporates continuous monitoring, periodic control validation, and executive oversight to ensure security risks remain within approved tolerance levels. Security controls are implemented commensurate with the sensitivity, classification, and business impact of the information assets they protect.

II. Purpose

The purpose of this program is to define the administrative, technical and physical safeguards implemented to protect Personally Identifiable Information (PII) customer data employee information confidential business information, and systems supporting business operations.

This Program establishes a structured methodology for identifying, assessing, mitigating, monitoring, and reporting information security risks. It defines governance accountability, control ownership, risk tolerance thresholds, and oversight mechanisms to ensure consistent and measurable protection of information systems and sensitive data.

This document serves as the governing authority for cybersecurity activities across the organization. protections.

III. Scope

The Information Security Program will establish standards addressing administrative, technical, and physical safeguards in order to (1) ensure the security and confidentiality of protected records and information; (2) protect against any anticipated threats or hazards to the security or integrity of such data; (3) protect against unauthorized access to or use of such records or information which could result in substantial harm or

inconvenience to Dynatron Software and/or Dynatron Software clients or partners; (4) ensure the proper disposal of protected information and consumer information; and (5) provide appropriate response to unauthorized access to or use of sensitive information or information systems.

This program should be taken as part of a cybersecurity framework that includes the documented policies, controls, procedures, standards, and guidelines attached herein as "Appendix A".

This Program applies to all employees, contractors, third parties, cloud-hosted systems, on-premises systems, remote access environments, and any information systems that store, process or transmit Dynatron Software or client data. The Program governs the full data lifecycle including collection, processing, transmission, storage, archival, and destruction.

IV. Executive Oversight

The Executive Team and Board of Directors are aware of their responsibility to comply with applicable laws and regulations governing the protection of sensitive information and support the Cybersecurity Program in the development, implementation, and maintenance of the provisions of the written information security program and related activities. Hence, the Executive Authority accountable for Cybersecurity shall, at a minimum, report annually to the Board of Directors on the implementation, administration, maintenance, and effectiveness of the Cybersecurity program. Such reports may be made more frequently or on an as-needed basis at the discretion of the Executive Team. Executive reporting may include, at a minimum: results of annual risk assessments; status of remediation activities and open risk items; incident trends and root cause summaries; vulnerability and patch management metrics; third-party risk assessment status; and results of security control testing and audits.

V. Information Security Policies, Procedures, and Controls

The Executive Team has approved/delegated to Cybersecurity Leadership, to set policy statements and to guide management in the development of detailed procedures for the implementation of information security controls. Any Cybersecurity Policy and/or Governance documentation which is controlled, approved, and maintained by Cybersecurity Leadership, are to be considered an Addendum to this Information Security Program document.

The Cybersecurity Senior and Executive Leadership are the designated owner of this Information Security Program. The Program shall be reviewed at least annually and upon significant regulatory, organizational, or technological change. Updates shall be documented in the Version Control section and approved by appropriate leadership.

Information Security Controls shall be developed by the Cybersecurity organization to guide the development of formally documented procedures and to assist planning for testing and audit of the effectiveness of the Information Security Program.

Dynatron Software recognizes that the creation of effective Cybersecurity programs and policies require efforts beyond the IT Department and must encompass other aspects of organizational operations. All departments and business units are therefore directed to include language within project management procedures to coordinate with staff responsible for information security during all phases of the acquisition process for systems, applications, or third-party information services, including selection, evaluation, and contracting.

VII. APPROVAL

Dynatron Software Cybersecurity Leadership shall annually review the Information Security Program to ensure accuracy and applicability. This Program supersedes all previously established policies and all other material in conflict with its provisions.

Dynatron

VIII. Related Documents

- Dynatron Software: “Employee Handbook”;
- Software Installation Policy
- Security Awareness Training and Testing Policy
- AI Usage Policy
- Acceptable Use Policy
- Data Classification Policy
- Data Retention Policy
- Third Party Risk Management Policy
- Access Management Policy
- Change Management Policy
- BYOD Policy
- Encryption Policy
- Logging Policy
- Patch Management Policy

APPENDIX A – INFORMATION SECURITY POLICIES

1. **Compliance with laws and regulations**: Dynatron Software will comply with all applicable laws and regulations governing Cybersecurity and the protection of data therein.

2. **Exceptions to policies and procedures:** Information security procedures and policies shall provide for circumstances under which exceptions to the documented policies or procedures may be necessary due to urgent need, such as business critical functions for customer or revenue producing issues, emergency break fix, level of effort for permanent remediation, etc. Exceptions shall be documented and closely monitored so as to ensure that information security controls or pertinent procedures are restored as soon as practicable. In the event that a specific Cybersecurity Policy or Program does not explicitly provide for an exception to that policy, the Cybersecurity team should be engaged via a documented ticket in the approved ticketing system for Dynatron, and the Team shall facilitate guidance and completion of the appropriate exception process for the issue being presented. All exceptions should be considered temporary until a permanent solution which is compliant to policy can be implemented. These exceptions shall be accounted for and reviewed quarterly as part of Cybersecurity's analysis of Dynatron's Risk Profile.

3. **Compliance oversight**: Cybersecurity Leadership is accountable for compliance monitoring through reports or other artifacts for affected environments and/or technologies on a schedule applicable to the environment and any requirements therein. Stakeholders and Environment owners will be responsible for providing required evidence and artifacts as requested by Cybersecurity.

4. **Responsibility for the Program**: The Cybersecurity Officer (CISO) or other qualified senior Cybersecurity Leadership in the absence of a CISO are responsible for the maintenance and execution of the Cybersecurity Program.

5. **Strategic planning of Information Security**: Cybersecurity Leadership shall meet with other executive and extended leadership members periodically to review pertinent Dynatron Software information security issues, risk treatment alternatives, and strategic planning for information security as it relates to the various business units within Dynatron. The Cybersecurity leader shall be a participant, and strategic Leader such planning exercises.

6. **Managerial responsibility:** Dynatron Software Managers and Directors shall take the initiative to ensure personnel within their departments understand Information Security Program guidance and rigorously follow pertinent information security procedures and Best Practices in accordance with all Cybersecurity Programs and Policies.

7. **Supplemental Guidance:** It is the expectation of Executive Leadership that Dynatron Software management, and in particular, Managers and Directors, to take

an active role to ensure attention to procedural detail within their departments.

8. **Executive leadership reporting and approval of risk management:** The executive leadership team, typically the Executive Leader/Sponsor to which the most senior Cybersecurity Leader (typically the CISO) report to, shall report to the CEO and Board of Directors, the overall status of the Cybersecurity program and compliance with the applicable policies and programs therein. The report shall address material risk issues, including specific activities within the previous year pertaining to risk assessment, risk management and risk treatment decisions, the process of determining a need and documenting approval for exceptions to risk treatments (controls), risk acceptance decisions, vendor/service provider management, control testing, security events that have triggered an incident response and data breaches, to include management responses to these issues as well as recommendations for changes in the Cybersecurity program.

9. **Vendor handling of information:** Dynatron Software shall perform risk assessments on all potential third-party vendors or providers, ensuring proper controls and contractual liabilities are in place before exposing the Environment, or data, to said vendors or providers.

10. **Risk Assessment:** At least annually, and prior to any service, infrastructure, or significant change in business processes involving sensitive information or information system, Management will perform an information security risk assessment in accordance with a formally documented procedure based on, and compliant with, any applicable compliance or framework requirements.

    Risk assessments shall follow a documented methodology incorporating defined criteria for likelihood and impact scoring. Risks shall be categorized (e.g., Low, Moderate, High, Critical), with residual risk evaluated against established risk tolerance thresholds approved by executive leadership. Risk acceptance decisions shall be formally documented and retained.

    Cybersecurity Leadership may (re)evaluate and adjust its risk assessment on a periodic basis and in light of any relevant changes in technology; changes in internal and external threats; changes in client base or service offering; and actual incidents of security breaches, identity theft, or fraud experienced by Dynatron Software or applicable industries.

11. **Asset Inventory:** An inventory of organizational assets (e.g., hardware, software, data, and systems hosted externally) is maintained where assets can be prioritized for protection based on the data classification and business value.

    - Each asset shall have an assigned business owner responsible for classification, protection requirements, and lifecycle management. Assets shall be categorized

according to data sensitivity and business criticality, and inventory reconciliation shall occur at least annually and following significant system changes.

Infrastructure Leadership has been designated made responsible for maintaining an inventory of organizational assets.

The asset inventory, including identification of critical assets, is reviewed at least annually to validate that new, relocated, repurposed, and sunset assets have been accounted for per process and policy adherence.

12. **Documentation of security controls:** Management shall formally document information security controls – managerial, operational and technical – implemented for the mitigation of risks, exposures and potential impacts. Formal procedures shall be documented to elaborate the steps necessary for implementation of the controls. Procedures shall specify the job position(s) responsible for their different elements, including execution, oversight, review, and updating. The documented controls shall be implemented with sufficient efficacy to reduce risks to acceptable levels. Implemented controls may be adjusted as needed to maintain information security risks within an acceptable range, taking account of risk assessment results and changes in the security environment.

13. **Testing and audit of information security controls:** Dynatron shall comply with any regulatory requirements, as well as Framework and Cybersecurity best practices, and conduct security assessments of all applicable environments, and Dynatron owned/developed software on at least an annual basis, with additional assessments being done as business needs warrant. Dynatron Software has achieved SOC 2 Type 1 attestation and is actively pursuing SOC 2 Type 2. External audit findings are remediated in accordance with the Vulnerability Management Program, with progress reported to executive leadership.

    Findings from the conduct of the Audit Plan and other audit activities, including any internal or external reviews or audits of the information security program and information security measures, will be remediated in accordance with the Vulnerability Management Program process and requirements, with exceptions following the Exception processes, and being accounted for in accordance with Risk Management process and policy.

14. **Employee security awareness:** Dynatron shall develop, implement, and manage a formal employee information security awareness training program that is designed to increase employees' awareness of information security threats and knowledge of information security controls. The training program should consider evolving and persistent threats and should include annual certification that personnel understand their responsibilities.

Annual certification and acknowledgment from the employee shall occur, with both the training syllabus (or lesson plan outline) and employee attendance documented. Annual information security training shall include incident response, current cyber threats (e.g., phishing, spear phishing, social engineering, and mobile security), and emerging issues.

Ongoing training shall be conducted and managed in accordance with Dynatron's Security Awareness Training Programs.

15. **User account management:** Dynatron shall document procedures for the management of user login accounts, as applicable for specific systems or environments, in compliance with related Policy, Procedure, Best Practice, or Compliance reporting guidelines. Administrative or Elevated Account Management shall have separate policies and guidelines as appropriate to comply with any specific requirements therein.

    User access shall be reviewed at least quarterly for systems containing sensitive or critical data. Access provisioning and deprovisioning shall follow documented approval workflows. Least privilege principles shall be enforced and validated during access reviews.

16. **Password management:** Dynatron shall document procedures to ensure that passwords and other authentication factors are utilized for all Dynatron Software information systems in accordance with the business impact, sensitivity and classification of the system and the data that it stores or processes, as outlined in applicable Policy or Compliance documentation.

17. **Change control:** Dynatron shall maintain a documented change management process governing infrastructure, cloud environments, security configurations, application deployments, and production systems. Emergency changes shall be documented, reviewed, and approved retrospectively to ensure appropriate oversight.

18. **System hardening:** Dynatron may establish procedures describing practices for securely configuring servers, workstations, network infrastructure, and security devices depending on the need and risk posture of the asset.

    The documented baseline may include all applicable access, audit, communication and other controls, and be designed according to "least privilege / least functionality" principles and apply specific required security features and functions. Exceptions to the documented baseline shall be corrected in a timely manner or documented with justification for the configuration requirement, as per applicable exception requirements.

19. **Vulnerability remediation:** Management may respond in a timely manner to security-related information system or application flaws that may be identified

through the various testing processes or reported incidents. The response may document a remediation plan, alternative mitigating controls in the case where remediation is not feasible or acceptance of the risk. These processes will follow requirements as outlined in the vulnerability management program, or other applicable processes, as documented by Cybersecurity.

20. **Patch management:** Dynatron will manage patch management as outlined in the vulnerability management process documentation.

21. **Malware protection:** Dynatron will utilize software, internal resources, and potentially external resources to detect, mitigate, and prevent malware.

22. **Physical Security:** Dynatron Leadership shall implement procedures describing how access to the workspaces, data center, and other sensitive areas is secured, controlled, and monitored.

    This will include implementing controls and procedures to address protections for computing (servers, workstations, network devices, printers, software) and non-computing (e.g., hardcopy document) assets.

23. **Personnel Security:** Dynatron Leadership will use employment job descriptions to address employee access to member information and shall implement practices for verifying job application information for all new hires.

    Contractors and third parties will be subject to confidentiality of the data accessed, business requirements, and acceptable risk.

    Managers and supervisors shall remain alert to changes in employees' personal circumstances that could increase the potential for system misuse or fraud. Management shall introduce practices to mitigate risk associated with an employee's termination, transfer or the imposition of sanctions.

    All employees will be required to sign appropriate access agreements prior to being granted access authorization to information systems or restricted areas and require all employees to review and sign this policy on an annual basis.

24. **Security monitoring:** Cybersecurity Leadership shall assign responsibility for monitoring employee compliance with security policies, procedures, and practices. The systems and environments monitored shall be identified in each applicable security procedure, policy, or program. Separate procedures shall also describe the monitoring of physical access to the facilities containing or providing access to the aforementioned systems.

    Cybersecurity shall employ technical and procedural means to detect and prevent intrusion into sensitive systems and information so as to reduce the likelihood or

impact of threat sources potentially compromising confidential or sensitive information.

Security logs shall be retained for a defined period consistent with regulatory, contractual, and business requirements. Monitoring alerts shall follow documented triage and escalation procedures to ensure timely investigation and resolution.

25. **Incident response:** Cybersecurity shall maintain and use an Incident Response Plan to be used in the event of security incidents. Cybersecurity Leadership is the default Incident Manager unless otherwise noted for specific circumstances within the Incident Response Plan. Only Cybersecurity Leadership can declare an incident after following documented procedure for Event and Incident analysis. In the event Cybersecurity Leadership cannot be engaged for said declaration, Cybersecurity's chain of command will consult with its executive leader, who will make said determination and declaration.

    To ensure effectiveness of incident response plans and employees' understanding of tasks and roles, training and test exercises may take the form of table-top paper scenario drills, penetration tests, or actual security incidents. Actual incidents may also serve as a test when the circumstances sufficiently invoke and execute the Incident Response Plan. Lessons-learned from each exercise shall be applied as applicable to the incident response process.

    Incidents shall be categorized by severity level. Post-incident reviews shall be conducted for incidents deemed material By Cybersecurity Senior and Executive Leadership to determine root cause and corrective actions. Regulatory and contractual notification obligations shall be evaluated as part of the response process.

26. **Data loss prevention:** Dynatron may adopt controls with associated implementation procedures to prevent data loss and supplement other security controls, detections and programs. Dynatron shall also have programs and methodologies in place to protect data in transit and at rest, as appropriate per data elements as they relate to any compliance, framework, or best practice requirements.

27. **Internet Access Management:** Cybersecurity may, if deemed appropriate for a particular role or department, implement technical and procedural controls to limit employee access to Internet sites associated with Dynatron Software related duties and away from websites known for or suspected of harboring malicious software, and other non-work-related websites. Filtering of network traffic employed for data loss prevention shall also be designed to prevent bypass of authorized access and the execution and spread of malicious program code.

28. **Wireless communications management:** The implementation of any wireless LAN or data communication devices shall require a documented risk assessment and risk management plan to be presented for approval prior to connectivity. Wireless LANs

shall be viewed as untrusted networks unless managed by Dynatron infrastructure with standard Dynatron security measures implemented, and therefore additional controls shall be implemented for Dynatron Software devices that connect to them.

29. **Remote Access:** Dynatron shall implement multi-factor authentication and other conditional access restrictions as deemed appropriate, as well as procedures that describe practices for the granting of approval, authentication, authorization, and monitoring of remote access users. Cybersecurity shall determine the requirements for VPN technology to be adopted as the remote access VPN standard.

30. **Multi-factor authentication:** (MFA) shall be required for remote access to production or sensitive environments. Conditional access controls shall be enforced where it is technically feasible to reduce unauthorized access risk.

31. **Media disposal:** Dynatron will identify the digital devices that store sensitive or confidential information and will ensure the disposal and destruction of the hardware and data therein comply with any applicable regulations, frameworks, best practices, and internal policy adherence.

32. **Service provider oversight:** Cybersecurity Leadership will establish and maintain due diligence policies and procedures for service provider oversight in order to minimize the risk of unanticipated costs, legal disputes and asset losses and to ensure the security and confidentiality of protected information.

    Dynatron Software's service provider oversight process may include guidance for Risk Assessment of potential providers. Prior to engaging in a proposed activity, Dynatron Software will perform a risk assessment to determine whether the relationship complements the organization's overall mission and philosophy, and if the proposed activities, related costs, product and services standards, and third-party involvement are consistent with the overall business strategy and risk tolerances.

33. **Backup and restore:** Cybersecurity Leadership will delegate responsibility to applicable business units to maintain a procedure describing the practice of periodic backup of system data and supporting networked systems. The procedure may specify backup schedule, documentation, and test restore requirements. This will include guidance on an alternate storage site that includes necessary agreements to permit the storage and retrieval of information system backup information and for information security safeguards equivalent to that of the primary site.

    Backup restoration exercises shall be performed at least annually and results documented. Backup data shall be protected using encryption and access controls equivalent to production systems.

34. **Business Continuity:** Cybersecurity Leadership will delegate responsibility to applicable business units to have documented plans and procedures for maintaining continuity of business services at acceptable levels.

    Stakeholders shall coordinate contingency plan development with organizational elements responsible for related plans and shall include measures to address various threat scenarios, natural and man-made, as identified through risk assessment exercises. The plan may be tested on a scheduled basis and adjusted based upon lessons learned through testing and actual events.

    Training will be provided to all personnel responsible for executing the contingency plan so that they understand and can execute their allocated duties.

    Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) shall be defined for critical systems. Business continuity plans shall be tested periodically and updated based upon lessons learned through testing and actual events.

35. **Acceptable use:** Cybersecurity Leadership shall document explicit guidelines for the acceptable use of Dynatron Software information systems and data. All employees shall be required upon initial employment and annually thereafter to sign an acknowledgement of having read, understood and agreed to abide by the guidelines. Employees are forbidden from disclosing confidential information or other Dynatron Software sensitive information to unauthorized persons or entities, as well as to authorized persons or entities without protective measures outlined in this program. Management shall have a policy to govern employees installing unauthorized software or hardware onto Dynatron Software information systems. Any employee found to have violated this program is subject to disciplinary action, up to and including termination of employment.

    Acceptable use guidelines shall include specifications for employee references to Dynatron Software affiliations and activities within any social media postings to ensure that Dynatron Software is appropriately represented in public forums.