Dynatron Software
Information Security Program

Date Issued	**10/12/20222**	
Supersedes Issuance Dated	**09/07/2020**	

Confidential

Version 1.1

This document supersedes all previous versions.

Dynatron Software

Document Control

Document Information

	Information
Document Id	Dynatron Software Information Security Program
Document Owner	Information Security Officer
Issue Date	**08/02/2022**
Last Saved Date	8/03/2022
File Name	

Document History

Version	Revision Date	Changes
1.0	07/13/2020	Document Created
2.0	07/20/2020	Revisions
3.0	8/10/2020	Updated Per Revisions
4.0	10/12/2022	Updated Per Revisions

Document Approvals

Role	Title
Document Sponsor	CTO
Analysis Review Parties	Security Steering Committee
Primary Analyzer	Dynatron IT Staff
Document Authority	Board of Directors

Approval Date

Version	Date	
1.0	**09/07/2020**	Executive Management / Security Steering Committee Approval Obtained
1.1	**10/12/2022**	Executive Management / Security Steering Committee Approval Obtained

I. Overview

Dynatron Software's business mission requires the effective protection of sensitive information and information systems in keeping with business needs and regulatory compliance. This Information Security Program is implemented to guide Dynatron Software management in managing information security risks while maintaining business operations.

II. Purpose

The purpose of this document is to provide guidance to Dynatron Software management in the creation and implementation of an Information Security Program designed to protect the confidentiality, security, and integrity of sensitive information and information systems in compliance with industry best practices and all applicable regulations, to include all Federal, State, and industry guidelines concerning the protection of Personally Identifiable Information (PII) and all other consumer and employee information 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 an information security framework that includes the documented policies, controls, procedures, standards, and guidelines attached herein as "Addenda A".

IV. Security Steering Committee

The Security Steering Committee is comprised of Stakeholders from the Executive Team, Operations Departments, and IT. The purpose of the Security Steering Committee is to review and prioritize all IT Project requests to ensure they are aligned with the business strategy and that resources are being used appropriately based on business needs, values, and goals.

The Security Steering Committee shall have the authority and responsibility, subject to the approval of the CEO, for the development and administration of a written information security program that equals or exceeds the information security standards prescribed by regulatory guidance and other applicable federal and state information security laws and regulations. The Security Steering Committee should, where appropriate, involve non-IT personnel throughout the organization to contribute to the overall risk management process to ensure thoroughness and maximum coverage of risk mitigation strategies.

V. Board Oversight

The Board of Directors are aware of their responsibility to comply with applicable laws and regulations governing the protection of sensitive information and oversee the Security Steering Committee in the development, implementation, and maintenance of the provisions of the written information security program and related activities as noted herein. Hence, the CTO shall, at a minimum, report annually to the Board of Directors on the implementation, administration, maintenance, and effectiveness of the information security program. Such reports may be made more frequently or on an as-needed basis at the discretion of the CEO, or as called upon by the Security Steering Committee.

VI. Information Security Policies, Procedures and Controls

The CEO has approved a set of policy statements to guide management in the development of detailed procedures for the implementation of information security controls. The Information Security Policies document is considered an Addenda to this Information Security Program.

Information Security Controls shall be developed by management and approved by the Security Steering Committee 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 information security requires 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. Related Documents

- Dynatron Software “Catalog of Applicable Information Security Controls,” V 0.90, June 2020;
- Dynatron Software: “Employee Handbook”;
- Dynatron Software: “IT-280520-1327-94”;
- Dynatron Software Data Policy;
- Dynatron Software: “IT_Project_Intake_Steering_Committee_Process”; and
- Dynatron Software: “IT Project Management Process”

VIII. Approval

Dynatron Software CTO shall annually submit the Information Security Program to the Board of Directors for formal approval. Changes to the Program are subject to approval by the CEO, and shall not be implemented until formal approval, except for those changes meeting exception requirements set forth in the Program.

This Program supersedes all previously established policies and all other material in conflict with its provisions.

Addenda A – Information Security Policies

1. **Compliance with laws and regulations**: Dynatron Software will comply with all applicable laws and regulations governing the safeguarding of Personally Identifiable Information (PII) and other protected information, including all applicable laws and regulations regarding the safeguarding of such information.

2. **Exceptions to policies and procedures:** Information security procedures shall provide for circumstances under which exceptions to the documented policies or procedures may be necessary due to urgent need, such as emergencies. Exceptions shall be documented and closely monitored so as to ensure that information security controls or pertinent procedures are restored as soon as practicable. Any exceptions to policies or procedures shall be reported with justification to the Security Steering Committee, on a quarterly basis.

3. **Compliance oversight**: The Information Security Officer is responsible for overseeing compliance monitoring through reports submitted by the Security Steering Committee.

4. **Responsibility for the Program**: Management responsibility for the Information Security Program shall be delegated to the Information Security Officer a person formally appointed to that position by the CEO.

5. **Strategic planning of Information Security**: The Security Steering Committee shall convene periodically to deliberate over pertinent Dynatron Software information security issues, risk treatment alternatives and strategic planning for information security. The Information Security Officer shall be a member of the Security Steering Committee. Management reports to the Security Steering Committee should make use of metrics, measurable details about the operation of controls, in order to inform the committee more comprehensively on the functioning and effectiveness of the controls.

Supplemental Guidance: Security planning processes should make use of the knowledge of subject matter experts from throughout the organization, such as stakeholders in critical business processes.

6. **Managerial responsibility:** Dynatron Software Managers & Directors shall take the initiative to ensure personnel within their departments understand Information Security Program guidance and rigorously follow pertinent information security procedures.

Supplemental Guidance: The CEO expects Dynatron Software management, and in particular, Managers & Directors, to take an active role to ensure attention to procedural detail within their departments.

7. **CTO reporting and approval of risk management:** The CTO shall, at least annually, report to the CEO via the Security Steering Committee, and senior management the overall status of the information security program and compliance with the Guidelines. 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, controls 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 information security program.

All information security controls shall have features enabled to allow for testing and auditing for implementation and management effectiveness.

8. **Consumer information handling:** Information security policies regarding the proper disposal

of information also apply to personal information Dynatron Software obtains about individuals regardless of whether or not they are Dynatron Software customers or employees ("consumer information").

Supplemental Guidance: Consumer information includes, for example, any instance of PII collected during any business operation through Dynatron actions or associated third parties, to include marketing or sales activities.

9. **Vendor handling of information:** Dynatron Software shall require that providers of external information system services (e.g., Professional Services, Multi-Sourcing, IT Outsourcing, Process-Specific Outsourcing, Business Process Outsourcing, Local Outsourcing, Offshore Outsourcing and Nearshore Outsourcing) handling information comply with organizational information security requirements, directives, policies, regulations, standards, and guidance for the proper handling and disposal of that information.

   Management shall define and document oversight and user roles and responsibilities with regard to external information system services and monitor security control compliance by external service providers on an ongoing basis.

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.

    Management will 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.

    The risk assessment methodology should include processes to:

    - Assess the sufficiency of policies, procedures, information systems, and other arrangements in place to control identified risks;
    - Identify and determine the sensitivity of protected information;
    - Identify reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of confidential or sensitive information or systems handling such information; and,
    - Monitor, evaluate, and adjust its risk assessment practices and information security program in light of any relevant changes to technology, the sensitivity of information, and internal or external threats to information security.

    The risk assessment procedure shall be presented to CEO for approval. The procedure shall document a method for determining whether or not controls that have been implemented for the mitigation of vulnerabilities and business impacts may be considered to reduce the residual risk to an acceptable level. The results and findings of risk assessment activities shall also be presented to the Board of Directors to aid the CEO in carrying out necessary oversight and governance responsibilities.

    For residual risk in excess of acceptable levels and newly exposed critical vulnerabilities, Dynatron Software will develop a plan of action and milestones to document the remedial actions intended to remediate these risks and vulnerabilities. This plan will be updated quarterly based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.

    Supplemental Guidance: All information security procedures and risk management processes shall take account of the information learned and documented through risk assessment processes. Risk assessment processes should make use of the knowledge of subject matter experts from throughout the organization, such as stakeholders in critical business processes. Dynatron Software may choose to engage third-party expertise to assist in risk assessment processes.

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

    Dynatron Software Management has designated the IT Department as being responsible for maintaining an inventory of organizational assets.

    The asset inventory, including identification of critical assets, is updated at least annually to address new, relocated, re-purposed, and sunset assets.

12. **Classification of systems and data:** Data owned, used, created, or maintained by Dynatron Software is classified into the following three categories: Confidential, Sensitive, and Public. Management shall document a procedure to elaborate how these different categories of data shall be identified and handled. The classification may be supported by an assessment of risks from threats to the confidentiality, integrity and availability of the data.

13. **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 shall 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.

    Supplemental Guidance: Multiple controls may be implemented through one procedure. Similarly, certain controls may require multiple procedures in order to fully implement the control as defined. The development and maintenance of formally documented procedures to fully implement all attested controls is a substantial undertaking. Management effort should focus on the development / documentation of the procedures necessary to support those controls identified as most important / significant to organizational information security, with the ultimate goal of a complete and effective documentation to permit verification of the control through audit.

14. **Testing and audit of information security controls:** Testing and auditing of information security controls may be conducted at least annually as part of a 12-Month Audit Plan to be developed by the Security Steering Committee and submitted to the CEO.

    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, may be reported to the Board via the Security Steering Committee. Testing plans, and audit activities shall be conducted independently of IT staff as well as other departments. In addition to controls testing, audit plans shall include empirical technical tests, such as vulnerability assessment scans or penetration testing, on a periodic basis and under conditions appropriately controlled to avoid negative impacts to Dynatron Software business processes.

Controls testing and other empirical technical tests may serve as validation of the risk assessment process, in addition to providing a measure of effectiveness of individual controls implemented, controls management, and identification of potential control gaps.

For deficiencies and vulnerabilities revealed by testing, Dynatron Software will develop a plan of action and milestones to document the remedial actions intended to remediate these deficiencies and vulnerabilities. This plan may be updated [monthly, quarterly, other] based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities. Specific personnel will be assigned responsibility for executing each item in the plan of action and milestones.

Senior Management shall ensure that the security staff responsible for oversight of information security and other technical audit processes possess sufficient audit experience, expertise, and training in order to perform these functions.

15. **Employee security awareness:** Management 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.

    Training shall be conducted annually, 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.

    Type, frequency and focus of training shall be tailored to the job requirements of different groups of employees. Principles learned by employees during this formal training shall be periodically reinforced by management, using email, posters, discussions, slogans and other informal methods. Situational awareness materials will also be made available to employees when prompted by highly visible cyber events or by regulatory alerts.

    The information security awareness and training program shall emphasize the importance of user vigilance against malicious software, shall include coverage of responsibilities for reporting security incidents and observed information security deficiencies to appropriate supervisors, and shall include reportable activities to the Security Steering Committee.

    Dynatron will document and monitor individual information system training activities including basic security awareness training and specific information security training and will retain individual training records for a period of three (3) years.

16. **Separation of Duties:** Management shall consult with the CEO regarding security related activities requiring separation of duties and/or dual control and review sufficiency of coverage.

17. **Access control:** Management shall document procedures for the management of access to data, information systems and system functions by the different users, groups and automated processes acting on behalf of users and requiring access. Procedures shall address the provision of differential access to functions and data based on a need-to-know / need-for-access principle.

18. **User account management:** Management shall document procedures for the management of user login accounts. The procedures shall apply to all systems, applications and devices with user identification, authentication, and authorization capabilities.

19. **Password management:** Management 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.

    Access controls will include guidance on password complexity and limits to password attempts and reuse.

    All passwords will be encrypted in storage and in transit.

    Dynatron Software Security Steering Committee will review identification and authentication policies and procedures annually to evaluate their sufficiency. This will include consideration of authentication related findings from test exercises or actual events.

20. **Management of administrative account access:** Elevated privileges (e.g., administrator privileges) will be limited and tightly controlled (e.g., assigned to individuals, not shared, and require stronger password controls).

21. **Change control:** Management shall document a formal change control procedure for the management of network firewalls and other devices / applications determined by management to require the application of this control due to potential business impact.

    Change control procedures shall integrate with those for software development and acquisition, patch management and system hardening. The change control process shall also take into account how changes may suggest modifications to the Disaster Recovery Plan in order to maintain the ability to meet DRP goals. The procedures shall document a process to handle emergency and temporary software fixes. The change control procedures shall include processes for managing changes to hardware, operating systems, applications, compatibility and capacity planning. Procedures shall also describe practices to restore a previous configuration in the event a software modification adversely affects one or more systems.

    Dynatron Software Management shall require review of systems applicable for formal change management and review of change management procedures annually.

22. **System hardening:** Management may establish procedures describing practices for securely configuring servers, workstations, network infrastructure, and security devices. Among the measures employed, system hardening may include removing or disabling unnecessary network and operating system services, changing all default passwords, clear text protocols, SNMP community strings and other authentication factors, as well as disabling any ports, functions, protocols and services not required for business purposes prior to placing any computing system or device into production on business networks.

    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. The documented baseline may include specifications for positive security features that should be operational.

    Baseline configurations may be documented, formally reviewed by CTO at least annually or as circumstances warrant and as part of system component installations and upgrades and have agreed-upon sets of specifications for information systems or configuration items within those systems.

23. **Flaw remediation:** Management shall 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 shall document a remediation plan, alternative mitigating controls in the case where remediation is not feasible or acceptance of the risk. The remediation plan shall take account of change management requirements and support the use of metrics for necessary CEO reporting.

24. **Patch management:** Management shall introduce procedures that describe practices for implementing security patches and updates for servers, workstations, and network devices. Patch management processes shall take account of information derived through risk assessment and include testing patches prior to deployment according to system criticality and information security risk.

    Within reports to the Security Steering Committee, Management shall include metrics concerning the operation and effectiveness of patch management processes.

25. **Malware protection:** Management shall identify and utilize additional controls to prevent and detect the installation and operation of malicious software.

    Supplemental guidance: Anti-malware measures may include, but not be limited to:
    - Applications to identify and restrict viruses and virus-like behavior, spyware and adware;
    - Rootkit scanners;
    - Scans for Alternate Data Streams;
    - File integrity checks;
    - Intrusion detection systems;
    - Application white-listing; and
    - Application stack hardening tools.

    Management shall incorporate into Dynatron Software information security awareness and training programs the importance of user vigilance against malicious software.

26. **Physical Security:** Management 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:
    - Enforce physical access authorizations at entry/exit points to the facilities where the information system resides;
    - Verify individual access authorizations before granting access to the facility;
    - Control ingress/egress to facilities where the information system resides;
    - Maintain physical access audit logs;
    - Control access to areas within the facility officially designated as publicly accessible;
    - Escort visitors and monitor visitor activity;
    - Secure keys, combinations, and other physical access devices; and
    - Change combinations and keys when keys are lost, combinations are compromised, or individuals are transferred or terminated.

    The procedures shall address protections for computing (servers, workstations, network devices, printers, software) and non-computing (e.g., hardcopy document) assets.

27. **Personnel Security:** Management 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.

28. **Security monitoring:** Management shall assign responsibility for monitoring employee compliance with security policies, procedures, and practices. Management shall document formal procedures and implement processes for review of logged system events. The procedure shall address at a minimum the frequency of reviews determined as necessary for the mitigation of risk. The systems monitored shall be identified in the procedure. Security monitoring procedures shall also describe the monitoring of physical access to the facilities containing or providing access to the aforementioned systems.

    Specific events to be logged shall be documented by management, but shall include at a minimum the information necessary to establish what type of event occurred, when (date and time) the event occurred, where the event occurred, the source of the event, the outcome (success or failure) of the event, and the identity of any user/subject associated with the event. Should the logging process fail, the system will alert designated organizational officials and will stop generating audit records. The logging system will be synchronized with an authoritative time source.

    Management shall employ technical and procedural means to detect and prevent intrusion into sensitive systems and information so as to reduce the likelihood of threat sources compromising confidential or sensitive information. The number, placement, and configuration of devices or sensors shall be sufficient to provide adequate coverage consistent with the level of risk inherent to existing systems. Management shall incorporate intrusion detection/prevention device and/or sensor alerting and reporting into incident response procedures. As practicable, management shall establish pre-programmed responses to alerts and/or log events including escalation procedures.

    Management shall document the requirements for retention of security-related event logs. The log retention period shall be determined from information gained through risk assessment activities but shall be sufficient to support adequate forensic evidence of intrusions, internal abuse, and audit functions.

29. **Incident response:** Management shall introduce procedures that describe incident response practices to meet security incidents indicated by risk assessment and threat profiling exercises. Roles and responsibilities for incident response team members will be defined, and the response team will include individuals with a wide range of backgrounds and expertise, from many different areas within the institution (e.g., management, legal, public relations, as well as information technology). Management shall designate a single employee as team manager to be in charge of incident response in addition to a deputy team manager who assumes authority in the absence of the team manager.

    Management will ensure a formal backup and recovery plan exists for all critical business lines that describes how critical systems are backed up and restored in the event of loss or corruption of production data.

Management shall ensure tools and processes are in place to detect, alert, and trigger the incident response program, and ensure logging and auditing practices support appropriate detection of incidents, and investigative and forensic requirements.

Management shall introduce a methodology for tracking and documenting problems and incidents from inception to resolution.

Management shall document processes for necessary notification of affected customers or partners in accordance with provisions outlined in contractual agreements, applicable laws, and other pertinent regulatory guidance.

To ensure effectiveness of incident response plan 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 exercise the incident response process. Lessons-learned from each exercise shall be applied as applicable to the incident response process.

Management shall document lessons learned from test exercises and actual events, and institute processes for revising the incident response plan based on lessons learned.

30. **Data leak prevention:** Management shall adopt controls with associated implementation procedures to prevent data leakage. The measures shall include, at a minimum, filtering of network traffic being sent from internal Dynatron Software information systems to public networks, such as the internet, and filtering of inbound network traffic that may contain malicious program code, such as through email. Measures shall also include personnel and other technical controls.

31. **Protection of data at rest:** Management shall introduce procedures describing practices for storage and transportation of hardcopy confidential and sensitive information and physical media containing electronic confidential or sensitive information. Protection of data at rest shall be consistent with the sensitivity and classification of the data and the requirements of the Physical security policy.

    Management will require annual assessments of controls related to the storage of confidential data.

32. **Protection of data in transit:** Management shall introduce procedures describing practices for the protection of electronic confidential and sensitive information in transit. Confidential information shall not be transmitted or transported outside Dynatron Software information systems or restricted areas in un-encrypted form. Management shall, consistent with assessed risk to information, determine the need for encrypting stored and transmitted information and introduce procedures describing the practices involved with implementing and managing encryption controls.

    Management will require annual assessments of controls related to the transmission of confidential data.

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

Internet access is permitted only through Dynatron Software firewalls. Employees are not permitted to employ dial-up lines and an Internet Service Provider (ISP) to reach the Internet from computers located in Dynatron Software offices, without express approval of the CEO.

34. **Website Management:** Management shall establish benchmark infrastructure standards for website performance, monitor and measure the actual performance against the benchmark. The benchmark shall take account of any CEO established guidelines.

    Management shall document procedures for the management of Dynatron Software's web site content. The procedures shall specify the individuals authorized to post information to organizational web sites, measures to ensure that non-public information is not posted to public sites and review of proposed content prior to posting. The procedure shall also take into account the requirements of change management and systems development and acquisition policies.

    Management shall effectively plan, implement, and monitor the organization's web linking relationships. This includes situations in which Dynatron Software has a third-party service provider create, arrange, or manage its website. The methods adopted to manage the risks of a particular link shall be appropriate to the level of risk presented by that link.

35. **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 to the CEO for approval prior to connectivity. Wireless LANs shall be viewed as untrusted networks and therefore additional controls shall be implemented for Dynatron Software devices that connect to them.

36. **Remote Access:** Management shall implement multi-factor authentication systems and procedures that describe practices for the granting of approval, authentication, authorization, and monitoring of remote access users. Management shall approve the VPN technology to be adopted as the remote access VPN standard. The use of any dial-in modems on Dynatron Software systems shall require approval by management.

    All Remote Access privileges, including administrative access, shall be reviewed annually, by the Security Steering Committee or its specifically designated personnel.

37. **Media disposal:** Management will identify the digital devices that store sensitive or confidential information and will ensure the hard drive or flash memory is erased, encrypted or destroyed prior to being returned to the leasing company, sold to a third party or otherwise disposed of. Management shall submit to the Security Steering Committee for approval a recurring schedule authorizing the disposal of specific kinds of sensitive information. Management shall submit to the Security Steering Committee, and the Committee shall approve a list of records, documents, or files to be excluded from destruction.

38. **Systems development and acquisition**: Management shall introduce procedures that describe how new or modified networked applications that interface confidential or sensitive information are approved, prioritized, acquired, developed, and maintained, i.e., a systems development life cycle (SDLC) methodology. Management shall address risk assessment, security controls, audit trails, activity logs and potential impact to business continuity planning as part of the development or acquisition process.

    All organizational departments shall coordinate with the Security Steering Committee for all phases of acquisitions for any system, application or service that interfaces with confidential or sensitive data or is installed on a system that interfaces with member data. Such consultation shall be included during risk assessment, planning, evaluation, selection, and contracting.

39. **Service providers oversight:** Dynatron Software Management 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 shall include guidance for:

    - Risk Assessment: 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.
    - Vendor Classification: For the purpose of conducting appropriate risk assessments, due diligence and oversight of new and existing vendors, Dynatron Software will classify vendors into 3 tiers:
        - Critical
        - Significant
        - Non-Essential
    - Vendor Background Check: Management will research and/or interview prospective organizations to determine which is best qualified to meet Dynatron's business and information security needs.
    - Vendor Monitoring: Where indicated by risk assessment, Management will develop appropriate procedures to monitor its service providers to confirm that they maintain agreed upon information security controls.

40. **Backup and restore:** Management shall introduce a procedure describing the practice of periodic backup of system data and supporting networked systems. The procedure shall 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.

41. **Business Continuity:** Management shall develop documented plans and procedures for maintaining continuity of business services at acceptable levels.

    Management 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 shall 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.

42. **Acceptable use:** Management 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 prohibit employees from 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.

43. **System maintenance:** Management shall document procedures to address the controlled maintenance and repair of information systems and components to support the necessary confidentiality, integrity and availability requirements of Dynatron Software information systems, services and data.