



WBT Systems' Data Protection Plan


The goal of WBT Systems' Data Protection Plan is to ensure that the TopClass software product and the WBT Systems Hosting environments remain as secure as possible to prevent, limit or contain the impact of a potential cybersecurity event. In this way, we aim to protect the computing environments and data in all supported deployment configurations for all types of customers.

WBT Systems' Data Protection encompasses every phase of the product lifecycle, including the design, development, testing, maintenance, deployment and implementation of the TopClass product. While WBT Systems cannot mitigate every possible security risk, our primary security and privacy assurance focus is three-fold:

- **Reducing the incidence of security weaknesses in TopClass** by following Secure Coding Standards, requiring mandatory security training for developers, cultivating security leaders within development groups, and using automated analysis and testing tools.
- **Reducing the impact of security weaknesses in released TopClass versions on customers** by adopting transparent security vulnerability disclosure and remediation policies, committing to treating all customers equally, and delivering the best possible security hotfix experience.
- **Reducing the impact of security vulnerabilities in the WBT Systems Hosting infrastructure** by adopting transparent security vulnerability disclosure and remediation policies, committing to rapid response actions in the event of a cybersecurity event, and mitigating risk exposure as expeditiously as possible.

WBT Systems' Data Protection Plan is an integrated, organization-wide approach to managing cybersecurity risk. It provides context on how WBT Systems views cybersecurity risk and the processes in place to manage that risk. The Plan will be regularly updated based on the application of risk management processes to changes in WBT Systems' business/mission requirements and the evolving threat and technology landscape. The outline below generally describes WBT Systems' corporate goals and objectives, following the framework created by National Institute of Standards and Technology *Framework for Improving Critical Infrastructure Cybersecurity v1.1*, as published April 16, 2018 (the "NIST Cybersecurity Framework").

The NIST Cybersecurity Framework provides organization and structure to multiple approaches to cybersecurity by assembling technology-neutral standards, guidelines, and practices that are working effectively in industry today. The structure starts with five concurrent and continuous risk management functions (Identify, Protect, Detect, Respond, and Recover) and then elaborates the set of related activities and desired outcomes within each function. More detailed policies, procedures and internal



guidelines are referenced as appendices to this high-level plan but are kept confidential in a further effort to reduce cybersecurity risk.

Change History

Date	Changed by	Description of Changes	
06/20/2022	L Bowers	Initial version	
26/09/2023	L Bowers	Updated for AZURE migration	
26/11/2024	L Bowers	Minor Updates and formatting	

WBT Systems Data Protection Plan Framework

Identify

This section defines WBT Systems' corporate business context, identifying the resources that support critical WBT Systems functions, and describing the related cybersecurity risk thus enabling WBT Systems to focus and prioritize its efforts, consistent with its risk management strategy and business needs.

Asset Management

Identify and prioritize the data, personnel, devices, systems, and facilities that enable WBT Systems to achieve its business purposes and manage them consistent with their relative importance to WBT Systems' business objectives and risk strategy. Establish cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners).

Business Environment

Understand and prioritize WBT Systems' mission, objectives, stakeholders, and activities to inform cybersecurity roles, responsibilities, and risk management decisions.

Governance

Establish an information security policy and other policies, procedures and processes to manage and monitor WBT Systems' regulatory, legal, risk, environmental, and operational requirements.

Risk Assessment

Identify and document cybersecurity threats to WBT Systems' operations, organizational assets and individuals, including potential business impacts and likelihoods. Identify and prioritize risk responses.

Risk Management Strategy

Determine risk management processes and WBT Systems' risk tolerance based on WBT Systems' priorities, constraints, and assumptions as established and used to support operational risk decisions.

Supply Chain Risk Management

Establish WBT Systems' priorities, constraints, risk tolerances, and assumptions and use them to support risk decisions associated with managing supply chain risk. Implement the processes to identify, assess and manage supply chain risks.

Protect

This section describes WBT Systems' methods, means and appropriate safeguards to ensure delivery of products and services that will prevent, limit or contain the impact of a potential cybersecurity event.

Identity Management and Access Control

Limit physical and remote access to assets and associated facilities to authorized users, processes, or devices, and only for authorized activities and transactions. Manage access permissions, incorporating the principles of least privilege and separation of duties, and protect network integrity, incorporating network segregation where appropriate.

Awareness and Training

Provide cybersecurity awareness education and training to WBT Systems personnel to ensure they perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.

Data Security

Manage information and records (data) consistent with WBT Systems' risk strategy to protect the confidentiality, integrity, and availability of information. Protect data-at-rest and data-in-transit. Manage assets through removal transfers and dispositions. Implement protections against data leaks. Verify software, firmware and information integrity via integrity checking mechanisms. Separate the production environment from the development and testing environment(s).


Information Protection Processes and Procedures

Create, maintain and continuously improve security and privacy policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among WBT Systems entities), processes, and procedures to manage the protection of information systems and assets. Create and maintain a baseline configuration of information technology control systems. Implement a System Development Life Cycle to manage systems. Implement configuration change control processes. Conduct, maintain and periodically test information backups. Implement, manage and test response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery). Develop and implement a vulnerability management plan.

Maintenance

Maintenance and repair of information system components is performed and logged in a timely manner, with approved and controlled tools, and performed in a manner that prevents unauthorized access.

Protective Technology



Manage technical security solutions to ensure the security and resilience of systems and assets, consistent with related WBT Systems policies, procedures, and agreements. Determine, document, implement and review audit/log records. Protect removable media and restrict its use according to policy. Control access to systems and assets, incorporating the principle of least functionality. Protect communications and control networks.

Detect

This section describes how WBT Systems deploys corporate resources to conduct the appropriate activities necessary to identify the occurrence and timely discovery of a cybersecurity event.

Anomalies and Events

Detect anomalous activity (from a baseline of network operations and expected data flows for users and systems) in a timely manner and understand attack targets and methods and the potential impact of events. Establish incident alert thresholds.

Security Continuous Monitoring

Monitor the information security environment and organizational assets (including the network, physical environment and personnel) at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures. Monitor for unauthorized personnel, connections, devices and software and perform vulnerability scans.

Detection Processes

Maintain, test and continuously improve detection processes and procedures to ensure timely and adequate awareness of anomalous events.

Respond

This section describes what actions WBT Systems will take in response to a detected cybersecurity event to contain the potential impact.


Response Planning

Execute and maintain response processes and procedures to ensure timely response to detected cybersecurity events.

Communications

Coordinate response activities with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies, legal counsel, and forensic analysts.

Analysis



Conduct analysis to ensure adequate response and support recovery activities. Investigate detection system notifications, understand the impact of the incident, perform forensics and categorize incident consistent with response plans.

Mitigation

Perform activities to prevent expansion of the cybersecurity event, mitigate its effects and halt the incident. Mitigate any newly identified vulnerability or document it as an accepted risk.

Improvements

Update response plans and strategies to incorporate lessons learned from current and previous detection/response activities.

Recover

This section describes WBT Systems activities to support timely recovery to normal operations by restoring any capabilities or services that were impaired due to a cybersecurity event in order to reduce the event's impact.

Recovery Planning

Execute and maintain recovery processes and procedures to ensure timely restoration of systems or assets affected by cybersecurity events.

Improvements

Update recovery plans and processes to incorporate lessons learned from current and previous cybersecurity events.

Communications

Coordinate restoration activities with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other Computer Security Incident Response Teams (CSIRTs), and vendors. Manage public relations/reputational aspects. Communicate recovery activities to internal stakeholders and executive and management teams.



WBT Systems Data Protection Plan Implementation Appendices


A separate, accompanying document to this Plan consists of the detailed policies, procedures, standards, forms, and action plans required by WBT Systems' Data Protection Plan and corresponds to the primary areas of the NIST Cybersecurity Framework. This confidential document is targeted to WBT Systems staff for detailed implementation instruction and guidance. A list of these appendices and their contents is provided below:

APPENDIX A – IDENTIFY FUNCTION POLICIES AND PROCEDURES

- POLICY ROLES AND RESPONSIBILITIES
- THIRD PARTY SERVICE PROVIDERS AND THIRD PARTY AGREEMENTS
- RESPONSIBILITIES AS A SERVICE PROVIDER

APPENDIX B – PROTECT FUNCTION POLICIES AND PROCEDURES

- SECURITY AWARENESS AND ACCEPTABLE USE POLICY
- PERSONAL MOBILE DEVICE USAGE POLICY
- VENDOR ACCESS MANAGEMENT POLICY
- CUSTOMER USER ACCESS MANAGEMENT POLICY
- ROLE_BASED ACCESS CONTROL POLICY
- SHARED ACCOUNT POLICY
- THIRD PARTY SINGLE SIGN-ON POLICY
- IT CHANGE CONTROL POLICY
- USER AUTHENTICATION POLICY
- DATA CLASSIFICATION AND CONTROL POLICY
- DATA RETENTION AND DISPOSAL POLICY
- FIREWALL AND ROUTER SECURITY ADMINISTRATION POLICY
- SYSTEM CONFIGURATION POLICY
- VULNERABILITY MANAGEMENT POLICY

- 
- PATCH MANAGEMENT POLICY AND PROCEDURES
 - DETECTION OF ROGUE WIRELESS DEVICES POLICY
 - ANTI-VIRUS POLICY
 - BACKUP POLICY
 - ENCRYPTION POLICY
 - USAGE POLICY FOR CRITICAL TECHNOLOGIES
 - EMPLOYEE IDENTIFICATION POLICY
 - SECURE DEVELOPMENT POLICY
 - DATA PROTECTION RISK MANAGEMENT POLICY

APPENDIX C – DETECT FUNCTION POLICIES AND PROCEDURES

- LOGGING CONTROLS POLICY

APPENDIX D – RESPOND FUNCTION POLICIES AND PROCEDURES

- INCIDENT RESPONSE PLAN AND PROCEDURES
- TOPCLASS PRODUCT VULNERABILITY POLICY AND PROCEDURES
- DISASTER RECOVERY PLAN AND PROCEDURES
- BUSINESS CONTINUITY PLAN