**CONFIDENTIAL**

*Trojan Bricks*

CYBER SYSTEM SECURITY PLAN

**Approvals**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Xavia A Denson

**Table of Contents**

[1 System Description 3](#_Toc31801852)

[1.1 System Attributes 3](#_Toc31801853)

[1.2 System Description and Mission 3](#_Toc31801854)

[1.3 Security Requirements 3](#_Toc31801855)

[1.4 System Environment 4](#_Toc31801856)

[1.5 Network Diagram(s) 5](#_Toc31801857)

[1.6 Dependencies and Interconnections 6](#_Toc31801858)

[2 Plan of Action and Milestones 7](#_Toc31801859)

[3 Security Controls 8](#_Toc31801860)

[3.1 Access Management 8](#_Toc31801861)

[3.1.1 EXAMPLE: Account Management 8](#_Toc31801862)

[3.2 Personnel Security 9](#_Toc31801863)

[3.3 Security Awareness and Training 9](#_Toc31801864)

[3.4 Physical Security 9](#_Toc31801865)

[3.5 System Communication Protection 9](#_Toc31801866)

[3.6 Remote Access 9](#_Toc31801867)

[3.7 Change Management 9](#_Toc31801868)

[3.8 Malicious Software Protection 9](#_Toc31801869)

[3.9 Logging Configuration 9](#_Toc31801870)

[4 Cyber Security Incident Response Plan 10](#_Toc31801872)

[5 Recovery Plan 11](#_Toc31801873)

# System Description

## System Attributes

|  |  |
| --- | --- |
| **System Name** | Trojan Bricks Network |
| **Impact Categorization** | Availability = Low  Integrity = Low  Confidentiality = Moderate |
| **System Owner** | • Name: Lola Wolfe  • Title: President and CEO  • Agency: Trojan Bricks  • Address: 2302 Norbit Ln, Pawnee, IN 89255  • Phone Number: 888-888-8888  • Email Address: lxwolfe@tricks.io |
| **Security Manager** | Dwight Schruit |
| **Primary System Administrator(s)** | Ron Swanson  Bob Hope  Sun Tzu  Edward Snowden |
| **Primary System Users** | Trojan Bricks |

## System Description and Mission

Trojan Bricks, Inc. was formed in 1990 to provide cheap, interlocking building block toys for children and adults of all ages. They are a publicly traded company headquartered in Little Rock, Arkansas and employ approximately 100 employees. Their primary product is the Trojan Bricks toy line sold in multiple theme-based packages. They are looking to expand into robotics and plan to launch their first Netflix series this Fall.

## Security Requirements

|  |  |  |
| --- | --- | --- |
| **Requirement** | **Impact** | **Description** |
| Confidentiality | Med | No unauthorized access to data will be permitted. The unauthorized disclosure of data could cause possible loss of trust |
| Integrity | Low | No unauthorized modification or destruction of data will be permitted, because it could cause a loss in revenue. However, when our robotics operations start, potential impact could go to Moderate. |
| Availability | Low | No disruption to access will be permitted |

## 

## System Environment

The system comprises of a single Internet facing web server from which all marketing and purchases take place. The web server has a back end mysql database (i.e. Database Server). An Active Directory server is used to manage all employee and contractor accounts, and a file server exists for sharing documents throughout the company. A network diagram is shown below.

## Network Diagram(s)

![A close up of a device

Description automatically generated]()

# Plan of Action and Milestones

*Use this section to specify a plan of action to address unmet or partially met security control objectives or to track vulnerability mitigation.*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ***POAM ID*** | ***Security Control/Issue*** | ***Plan of Action*** | ***Responsible*** | ***Milestone Date*** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

# Security Controls

Security controls will be based on instruction from NIST 800-53 revision 4 and NIST 800-12 revision 1

## Access Control

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Account Management  |  |  | | --- | --- | | **Requirement:** | The organization will identify and select information system accounts to support organizational missions. Organization will establishes conditions for group and role membership. | | **Control Reference:** | *NIST 800-53, AC-2* | | **Last Review and Update:** | 2020-Feb-05 | | **Implementation:** | | | 1) Departments for the company will be:  1. Executive staff - Overall responsibility for leading the company  2. Engineering - Design and Engineering for the Toy Brick line  3. Accounting - Responsible for all financials within the company  4. Marketing -  5. Human Resources  2) Managers and supervisors will oversee and review users’ activities to enforce use of information system access controls. Consulting departments will be given their own folder containing limited permissions which will be decided by Admins and the Executive staff.  3)  System Owners (members of respective departments), in coordination with department members, for Trojan Brick operations  systems will; and Senior Member will coordinate with System owners, for systems operated on  behalf of the Trojan Bricks to ensure service providers:  a) Manage through a life cycle consisting of establishing, activating and modifying accounts,  periodically reviewing accounts, and disabling, removing, or terminating information  system accounts, defined as individual, group, system and role-based accounts defined  as administrator, application, guest and temporary.  b) Assign Account Managers to accomplish life cycle activities.  c) Identify and select the following types of system accounts to support Trojan Bricks  missions/business functions: individual, group, system, application, guest and temporary.  i) Group and role accounts will be treated the same as user accounts for processing  and applying controls (e.g., only providing minimum access needed), and  ii) Processes will be established for reissuing shared/group account credentials (if  deployed) when individuals are removed from the group.  d) Document within applicable system security plans a description of authorized system  users (i.e, public, Trojan Brick employees), criteria group and role accounts’ membership with  access privileges, and other applicable account attributes.  e) Have requests to create information system accounts approved by IOs.  f) Require System Administrators, Account Managers, managers and supervisors to adhere  to the following procedures regarding creating, enabling, modifying, disabling or  removing accounts:  (i) Disable all accounts and user IDs;  (ii) Update access control lists, mailing lists, etc.;  (iii) Collect all keys, badges and similar items;  (iv) Reconcile any financial accounts over which the individual had control;  (v) Properly secure or dispose of electronic records;  (vi) In the event an individual is removed, laid off or let go under unfriendly  termination, the above actions shall be completed immediately. In addition, the  user should be rotated to a non-sensitive position, if possible, before the  employee is notified that he or she will be terminated.  (vii) Accomplish these procedures in accordance with applicable personnel,  contractual and grant mechanisms; and  (viii) Refer to Information Security – Personnel Security Procedures for  requirements on personnel termination and transfer.  Figure 1: | | |  | | |

### Access Enforcement | Role Based Access Control

|  |  |
| --- | --- |
| **Requirement:** | This system gives employees or anyone else with access to the network permissions of what they can do to the network or on the network based on their role in the system |
| **Control Reference:** | *NIST 800-53, AC-3(7)* |
| **Last Review and Update:** | 2020-Feb-05 |
| **Implementation:** | |
| Users will be given roles and these roles will be used to determine what permissions they have. No member will be allowed to edit their own permissions. Users will be given full privileges for file sharing.  Figure 1: Roles of the Executive Staff Group  A screenshot of a cell phone  Description automatically generated  Figure 2: Roles of the Engineering Staff GroupA screenshot of a cell phone  Description automatically generated  Figure 3: Roles of the Accounting Staff Group  A screenshot of a cell phone  Description automatically generated  Figure 4: Roles of the Marketing Staff Group  A screenshot of a cell phone  Description automatically generated  Figure 5: Roles of the Human Resources Staff Group  A screenshot of a cell phone  Description automatically generated | |
|  | |
| Account Management | Disable of Inactive Accounts  |  |  | | --- | --- | | **Requirement:** | Automated mechanisms to support the management of information system accounts, terminates temporary and emergency accounts after a company-specified time period,  disables inactive accounts after a company-specified time, and has automated mechanisms to audit account creation, modification, disabling, and termination actions and to notify, as required, appropriate individuals | | **Control Reference:** | *NIST 800-53, AC-2(3)* | | **Last Review and Update:** | 2020-Feb-05 | | **Implementation:** | | | A script runs every 90 days on the Domain Controller to disable users. The following screen shots show the scheduled task and script use to disable users.    Figure 1: Scheduled Task  A screenshot of a cell phone  Description automatically generated  Figure 2: Contents of the Powershell Script Disabling Inactive Users and Contractors | | |  | | | |
| Unsuccessful Login  |  |  | | --- | --- | | **Requirement:** | This control applies regardless of whether the logon occurs via a local or network connection. Due to the potential for denial of service, automatic lockouts initiated by information systems are usually temporary and automatically release after a predetermined time period established by organizations. If a delay algorithm is selected, organizations may choose to employ different algorithms for different information system components based on the capabilities of those components. Responses to unsuccessful logon attempts may be implemented at both the operating system and the application levels. | | **Control Reference:** | *NIST 800-53, AC-7* | | **Last Review and Update:** | 2020-Feb-05 | | **Implementation:** | | | There will be a 30 minute lockout period after 7 attempts.  A picture containing screenshot  Description automatically generated  Figure 1: GPO for Password Policies | | |  | | | |
| Authenticator Management  |  |  | | --- | --- | | **Requirement:** | Organizations will change default content of authenticators prior to information system installation. | | **Control Reference:** | *NIST 800-53, IA-5* | | **Last Review and Update:** | 2020-Feb-05 | | **Implementation:** | | | When creating an account an Administrator or other higher position owner will verify that the box is checked to ensure the user will recreate their password upon initial log in.  A screenshot of a cell phone  Description automatically generated Authenticator Management | Change Authenticators Prior to Delivery  |  |  | | --- | --- | | **Requirement:** | Organization will enforce a minimum password complexity of [Assignment: organization-defined requirements for case sensitivity, number of characters, mix of upper-case letters, lower-case letters, numbers, and special characters, including minimum requirements for each type];  Enforces password minimum and maximum lifetime restrictions of [Assignment: organization-defined numbers for lifetime minimum, lifetime maximum];  Prohibits password reuse for [Assignment: organization-defined number] generations; and | | **Control Reference:** | *NIST 800-53, IA-5(1)* | | **Last Review and Update:** | 2020-Feb-05 | | **Implementation:** | | | A GPO will be used to define password requirements  *Figure 1: GPO for Password Requirements*  A screenshot of a cell phone  Description automatically generated | | | | | |

## System Communication Protection

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Boundary Protection  |  |  | | --- | --- | | **Requirement:** | Subnetworks will be physically or logically separated from internal networks are referred to as demilitarized zones or DMZs. Restricting or prohibiting interfaces within organizational information systems includes, for example, restricting external web traffic to designated web servers within managed interfaces and prohibiting external traffic that appears to be spoofing internal addresses. Organizations consider the shared nature of commercial telecommunications services in the implementation of security controls associated with the use of such services. | | **Control Reference:** | *NIST 800-53, SC-7* | | **Last Review and Update:** | 2020-Feb-05 | | **Implementation:** | | | There will be firewall policies written to allow traffic to go to all internal server (File, Database, and Active Directory) using DNS and ICMP Protocols.  A screenshot of a cell phone  Description automatically generated  Figure 1: Firewall Rules | | | Boundary Protection  |  |  | | --- | --- | | **Requirement:** | This control enhancement applies to both inbound and outbound network communications traffic. A deny-all, permit-by-exception network communications traffic policy ensures that only those connections which are essential and approved are allowed. | | **Control Reference:** | *NIST 800-53, SC-7 (5)* | | **Last Review and Update:** | 2020-Feb-05 | | **Implementation:** | | | All ports will be closed off except those identified as necessary to be open.  A screenshot of a cell phone  Description automatically generated  Figure 1: Ports closed | | | | |

|  |
| --- |
|  |
| Cryptographic Key Establishment  |  |  | | --- | --- | | **Requirement:** | The organization establishes and manages cryptographic keys for required cryptography employed within the information system.  Key lifecycle:  1. Creation. A key is created on at least one domain controller, but its attributes (such as key value)  are not set.  2. Initialization. The key object has all its key attributes set on a domain controller.  3. Full Distribution. An initialized key is available to all domain controllers.  4. Active. An initialized key is available for all cryptographic operations on at least one domain controller.  5. Inactive. An initialized key is unavailable for some cryptographic operations on all domain controllers.  6. Termination. An initialized key is permanently deleted from all domain controllers | | **Control Reference:** | *NIST 800-53, SC-12* | | **Last Review and Update:** | 2020-Feb-05 | | **Implementation:** | | | New certificates will be generated through FortiGate’s certificate generator and distributed, as necessary.  A screenshot of a cell phone  Description automatically generated  Figure 1: Certificate generator | |  CRYPTOGRAPHIC OR ALTERNATE PHYSICAL PROTECTION  |  |  | | --- | --- | | **Requirement:** | Cryptographic mechanisms will be implemented to protect information integrity include. | | **Control Reference:** | *NIST 800-53, SC-8(1)* | | **Last Review and Update:** | 2020-Mar-15 | | **Implementation:** | | | Computers will maintain the setting to use TCP/IPv4 and DNS address  A screenshot of a cell phone  Description automatically generated  Figure 1: TCP/IPv4 Enable | | |
|  |

## Malicious Software Protection

### Flaw Remediation

|  |  |
| --- | --- |
| **Requirement:** | Organizations will identify information systems affected by announced software flaws including potential vulnerabilities resulting from those flaws, and report this information to designated organizational personnel with information security responsibilities. Organizations will also address flaws discovered during security assessments, continuous monitoring, incident response activities, and system error handling.. Organization-defined time periods for updating security-relevant software and firmware may vary based on a variety of factors including, for example, the security category of the information system or the criticality of the update. Organizations determine the degree and type of testing needed for the specific type of flaw remediation activity under consideration and also the types of changes that are to be configuration-managed. |
| **Control Reference:** | *NIST 800-53, SI-2* |
| **Last Review and Update:** | 2020-Feb-05 |
| **Implementation:** | |
| Flaw remediation actions that will be tracked and verified include, for example, determining whether organizations follow US-CERT guidance and Information Assurance Vulnerability Alerts. Organizations will also consider in testing decisions, whether security-relevant software or firmware updates are obtained from authorized sources with appropriate digital signatures. Lastly organizations will take advantage of available resources such as the Common Weakness Enumeration (CWE) or Common Vulnerabilities and Exposures (CVE) databases in remediating flaws discovered in organizational information systems.  Organizations will:  a. Identify, reports, and corrects information system flaws using commands such as “*get-hotfix"*  b. Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation (see SI-2(3)).  c. Installs security-relevant software and firmware updates within a given time (see SI-2(3)). | |

### Time to Remediate Flaws

|  |  |
| --- | --- |
| **Requirement:** | Organizations will determine the current time it takes on the average to correct information system flaws after such flaws have been identified, and subsequently establish organizational benchmarks such as time frames for taking corrective actions. Benchmarks will established by type of flaw and/or severity of the potential vulnerability if the flaw can be exploited. |
| **Control Reference:** | *NIST 800-53, SI-2(3)* |
| **Last Review and Update:** | 2020-Feb-05 |
| **Implementation:** | |
| IT personel will look at patches that will be released the second Tuesday of every month (commonly known as patch Tuesday) by visiting <https://docs.microsoft.com/en-us/windows/release-information/windows-message-center> and reading about upcoming releases. The personnel will then apply updates to a controlled group and after a 48-hour period, the updates will be applied to the rest of the clients.  Figure 1: Test Group  A screenshot of text  Description automatically generated | |

### Automated Mechanism

|  |  |
| --- | --- |
| **Requirement:** | The organization installs server software automatically. |
| **Control Reference:** | *NIST 800-53, SI-2(5)* |
| **Last Review and Update:** | 2020-Feb-05 |
| **Implementation:** | |
| Security and software updates to the server will be enabled to apply automatically.  Figure 1: Enable Automatic Updates  A screenshot of a cell phone  Description automatically generated | |

### Removal of Previous Versions

|  |  |
| --- | --- |
| **Requirement:** | Administrators will remove previous versions of software and/or firmware components that are not removed from the information system after updates have been installed, because they may be exploited by adversaries. |
| **Control Reference:** | *NIST 800-53, SI-2(6)* |
| **Last Review and Update:** | 2020-Feb-05 |
| **Implementation:** | |
| 1. Personnel may also accomplish this by creating a Group Policy that runs a script to delete the older version of the software/firmware. 2. Personnel may accomplish this by selecting an option to remove a previous version to uninstall previous version of a software/firmware when installing a new software/firmware.   Figure 1: Script to delete older version  A screenshot of a cell phone  Description automatically generated  Figure 2: Where to find software version  A screenshot of a cell phone  Description automatically generated | |

### Malicious Code Protection

|  |  |
| --- | --- |
| **Requirement:** | The organization will employ malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code. They will update malicious code protection mechanisms whenever new releases are available in accordance with organizational configuration management policy and procedures. They will also configure malicious code protection mechanisms. The organization will address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system |
| **Control Reference:** | *NIST 800-53, SI-3* |
| **Last Review and Update:** | 2020-Feb-05 |
| **Implementation:** | |
| 1. Perform periodic scans of the information system and real-time scans of files from external sources. For this organization, it will be the scanning tool in FortiGate.  2. FortiGate will also block virus’ in response to malicious code detection; and  3. The organization will carefully consider results that come from scan to not negatively impact information systems by reacting to false positives.  Figure 1: Antivirus incorporated into FortiGate  A screenshot of a cell phone  Description automatically generated | |

### Updates Only by Privileged Users

|  |  |
| --- | --- |
| **Requirement:** | Updates will only be applied when selected/approved by designated organizational personnel i.e. Administrators. |
| **Control Reference:** | *NIST 800-53, SI-3(4)* |
| **Last Review and Update:** | 2020-Feb-05 |
| **Implementation:** | |
| Updates will only be done through Group Policy to which only authorized personnel have access.  Figure 1: Updates by Administrators Only  A screenshot of a cell phone  Description automatically generated | |

### Malicious Code Analysis

|  |  |
| --- | --- |
| **Requirement:** | Employs contractors to analyze the characteristics and behavior of malicious code and incorporates the results from malicious code analysis into organizational incident response and flaw remediation processes. |
| **Control Reference:** | *NIST 800-53, SI-3(10)* |
| **Last Review and Update:** | 2020-Feb-05 |
| **Implementation:** | |
| Contractors will routine weekly scans on server and analyze the results.  Figure 1: Security Scan  A screenshot of a cell phone  Description automatically generated | |

### Authenticate Remote Commands

|  |  |
| --- | --- |
| **Requirement:** | This control enhancement protects against unauthorized commands and replay of authorized commands. This capability is important for those remote information systems whose loss, malfunction, misdirection, or exploitation would have immediate and/or serious consequences. |
| **Control Reference:** | *NIST 800-53, SI-3(9)* |
| **Last Review and Update:** | 2020-Feb-05 |
| **Implementation:** | |
| VPNs will be authenticated through the use of RADIUS (Remote Authentication Dial In Service).  Figure 1: Network Policy Server  A screenshot of a social media post  Description automatically generated | |

### Detect Unauthorized Commands

|  |  |
| --- | --- |
| **Requirement:** | This control enhancement can also be applied to critical interfaces other than kernel-based interfaces, including for example, interfaces with virtual machines and privileged applications. |
| **Control Reference:** | *NIST 800-53, SI-3(8)* |
| **Last Review and Update:** | 2020-Feb-05 |
| **Implementation:** | |
| IT contractors will monitor security logs to ensure that no unauthorized commands that have been set by the organization have been attempted.  Figure 1: Security Logs  A screenshot of a cell phone  Description automatically generated | |

## Logging Configuration

### Audit and Accountability | Audit Events

|  |  |
| --- | --- |
| **Requirement:** | An event is any observable occurrence in an organizational information system. Organizations define audit events as those events which are significant and relevant to the Trojan Bricks organization and the security of information systems and the environments in which those systems operate to meet specific and ongoing audit needs. The organization will identify audit events and keep record of them for a specified time. |
| **Control Reference:** | *NIST 800-53, AU-2* |
| **Last Review and Update:** | 2020-Feb-05 |
| **Implementation:** | |
| Audit events will include, for example, password changes, failed logons, or failed accesses related to information systems, administrative privilege usage, and third-party credential usage. This will be accomplished through a GPO that will maintain logs and not allow guest users to use certain applications.  A screenshot of a cell phone  Description automatically generated  Figure 1: Setting the size for max application log  A screenshot of a cell phone  Description automatically generated  Figure 2: Setting the size for max system log  A screenshot of a cell phone  Description automatically generated  Figure 3: Setting the length of time to retain the logs of applications  A screenshot of a cell phone  Description automatically generated  Figure 4: Setting the length of time to retain the security logs  A screenshot of a cell phone  Description automatically generated  Figure 5: Setting the length of time to retain the system logs | |

# 

# Cyber Security Incident Response Plan

<*This maps to control family IR. It is included outside of the security controls section because it is useful for individuals to quickly find in an event of a cyber security incident.*

*For the project provide a few paragraphs of things you would need to consider when responding to an incident. This does not need to be comprehensive.*>

# Recovery Plan

The security team will do monthly backups of the servers. Theses backups will be on tapes and the tapes will be stored off-site. In case of an emergency the hard backups will be used to recover data.

In case of querentine, laptops will be available for check out for those considered critical that do not also have company laptops. This laptops will have access to the VPN.