Allison Manning

20 Mar 2024

TABLE OF CONTENTS

1. SYSTEM IDENTIFICATION

1.1. System Name/Title: Design World Cloud Solution

1.1.1. System Categorization: Moderate Impact for Confidentiality

1.1.2. System Unique Identifier: A3CDW001

1.2. Responsible Organization:

Name:	Design World
Address:	1 HomeWorld Drive, San Diego, CA 92110
Phone:	619 502 5022

1.2.1. Information Owner (Government point of contact responsible for providing and/or receiving CUI**):**

Name:	Daniel Mercer
Title:	Information Owner
Office Address:	1 HomeWorld Drive, San Diego, CA 92110
Work Phone:	(619) 502-5022
e-Mail Address:	dmercer@designworld.com

1.2.1.1. System Owner (assignment of security responsibility)**:**

Name:	Daniel Mercer
Title:	Information Owner
Office Address:	1 HomeWorld Drive, San Diego, CA 92110
Work Phone:	(619) 502-5022
e-Mail Address:	dmercer@designworld.com

1.2.1.2. System Security Officer:

Name:	Carla Brooks
Title:	System Security Officer
Office Address:	1 HomeWorld Drive, San Diego, CA 92110
Work Phone:	(619) 502-5022
e-Mail Address:	cbrooks@designworld.com

1.3. General Description/Purpose of System

Design World's cloud solution facilitates secure, remote engineering and design work across multiple international locations. The system supports artistic structural support system design within a private cloud environment. It utilizes VPN access for secure remote connectivity, allowing employees to work in virtualized desktop environments without data leaving the secure, protected cloud.

1.3.1. Number of end users and privileged users

Design World's global operation of 100 employees focused on design and engineering, along with marketing and business management, the breakdown is as follows:

Number of Users	Number of Administrators/ Privileged Users
Number of Users: 80 ● Engineers and Designers: 60 ● Marketing and Business Management: 20	Number of Administrators/Privileged Users: 20 ● System Administrators: 10 ● Database Administrators: 5 ● Application Administrators: 5

1.4. General Description of Information

The system processes, stores, and transmits intellectual property related to Design World's engineering and design work. This includes proprietary designs and related information which are critical to the company's business and have been targeted by piracy and hacking efforts in the past.

2. SYSTEM ENVIRONMENT

The Design World cloud solution is designed to support secure, collaborative engineering and design work across global locations. The system architecture is centered around a private cloud infrastructure, enabling remote work and secure information sharing.

2.1. System Topology Narrative

The network consists of 15 hardware devices, structured as follows:

- **Subnets**
  Devices are organized within two distinct subnets.
- **Internet Access**
  A single device functions as the default gateway, controlling access to both subnets and the internet.

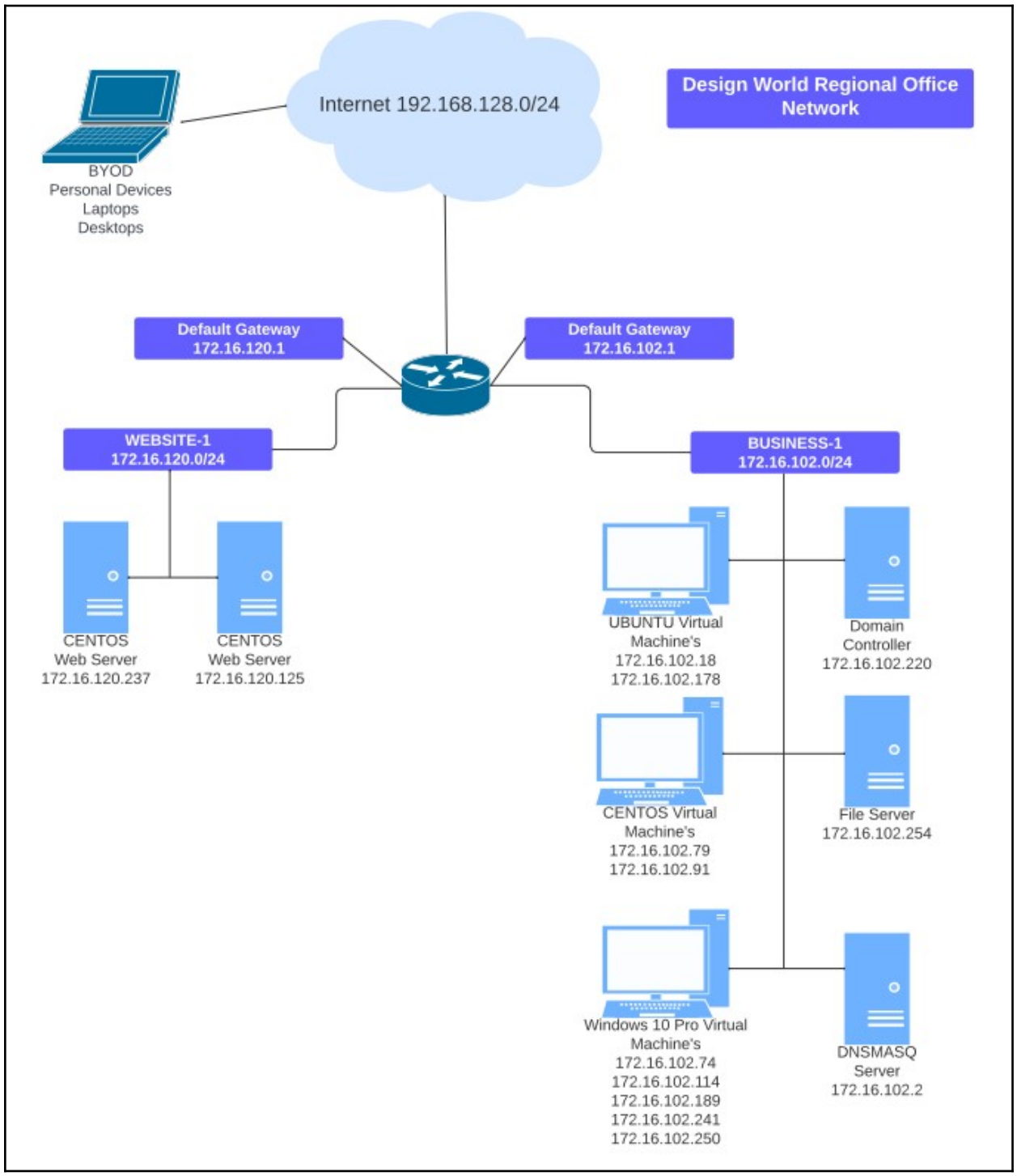
Hardware Breakdown

- **WEBSITE-1**
  - 2 CentOS Web Servers
- **BUSINESS-1**
  - 5 Windows 10 Pro workstations
  - 2 CentOS workstations
  - 2 Ubuntu workstations
  - 1 DNSmasq Server
  - 1 Windows Server 2016 File Server (FS)
  - 1 Windows Server 2016 Domain Controller (DC)

The Domain Controller (DC) is responsible for providing authentication and authorization functionalities for resources within the network.

- **Network Management**
  Network traffic across "WEBSITE-1", "BUSINESS-1", and the internet is managed by a single router.
- **Remote Connectivity**
  Users access the Design World cloud environment from their devices via a Virtual Private Network (VPN).

2.2. System Topology Diagram



2.3. Hardware Components

Hardware Components	
CentOS 7	**DW-WIN10-4**
IP: 172.16.102.79 MAC Address: FA:16:3E:2D:A1:1D	IP: 172.16.102.189 MAC Address: FA:16:3E:A9:49:86 OS: Microsoft Windows 10 CN=DW-WIN10-4.designworld.com
CentOS 7	**DW-WIN10-5**
IP: 172.16.102.91 MAC Address: FA:16:3E:53:AA:08	IP: 172.16.102.241 MAC Address: FA:16:3E:6C:B9:C5 OS: Microsoft Windows 10 Pro CN=DW-WIN10-5.designworld.com
CentOS Web Server	**File Server**
IP: 172.16.120.125	Netbios Name : DW-FS-OL2 IP: 172.16.102.254 MAC Address: FA:16:3E:B8:B5:E0 OS: Microsoft Windows Server 2016 CN=DW-FS-OL2.designworld.com
CentOS Web Server	**Ubuntu**
IP: 172.16.120.237	IP: 172.16.102.18 MAC Address: FA:16:3E:31:D6:EF mDNS hostname: dw-u20-2-ol2.local.
Domain Controller	**Ubuntu**
Netbios Name: DW-DC-OL2 IP: 172.16.102.220 MAC Address: FA:16:3E:A0:F0:54 OS: Microsoft Windows Server 2016 Standard Evaluation Build 14393 CN=DW-DC-OL2.designworld.com	IP: 172.16.102.178 MAC Address: FA:16:3E:FD:53:50 mDNS hostname: dw-u20-1-ol2.local.
DW-WIN10-1	**Router**
IP: 172.16.102.114 MAC Address: FA:16:3E:00:7F:18 OS: Microsoft Windows 10 CN=DW-WIN10-1.designworld.com	IP: 172.16.120.1 IP: 172.16.102.1
DW-WIN10-2	**DNSmasq Server**
IP: 172.16.102.250 MAC Address: FA:16:3E:3E:90:4F OS: Microsoft Windows 10 CN=DW-WIN10-2.designworld.com	IP: 172.16.102.2
DW-WIN10-3	
IP: 172.16.102.74 MAC Address: FA:16:3E:60:59:2E OS: Microsoft Windows 10 CN=DW-WIN10-3.designworld.com	

2.4. Software Components

Software Components
Curl-7.29.0-59.el7
DNSmasq
Firefox-115.4.0-1.el7_9
Fortinet 7.4
Freerdp-libs-2.0.0-4.rc4.el7_8
JDK 21
Linux Kernel 2.6
Linux Kernel 3.10.0-1127.el7.x86_64 on CentOS Linux release 7.8.2003 (Core)
Microsoft .NET
Microsoft Internet Explorer 11
Microsoft Terminal Services
Microsoft Windows 10 Pro
Microsoft Windows Defender
Microsoft Windows Server 2016 Standard Evaluation Build 14393
Microsoft Windows RPC
Microsoft Windows Kerberos
Microsoft Windows netbios-ssn
Microsoft Windows Active Directory LDAP
Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
OpenSSH 9.7
OpenSSL 3.2
Powershell 7
Python 3.9.19
Simple DNS Plus
TLS 1.3
Ubuntu 23.10

2.5. Hardware and Software Maintenance and Ownership

All hardware and software are maintained and owned by Design World. Design World has established contracts with service providers for the maintenance of its cloud environments and the licensing of all software used within the organization. This ensures that all components of the system are up-to-date, secure, and fully supported.

3. REQUIREMENTS

A3C's Information System Security Plan (ISSP) aligns with NIST Special Publication 800-171, December 2016. For each security requirement, we detail:

1. Requirement number and description,
2. Implementation status or plans,
3. Scoping guidance or compensating mitigations, if applicable. For non-applicable requirements, we provide rationale. This structured approach ensures our security measures meet industry standards efficiently.

Identifier	Security Requirement	DesignWorld Implementation
3.1 Access Control		
3.1.1	Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).	DesignWorld's access control policy leverages the utilization of a centralized identity management system, meticulously defining permitted account types. Furthermore, it implements robust role-based access controls to precisely align access restrictions with the delineated roles and responsibilities of users. Additionally, it provides explicit guidance on remote access protocols and procedures.
3.1.2	Limit system access to the types of transactions and functions that authorized users are permitted to execute.	DesignWorld's access control policy leverages the utilization of a centralized identity management system, meticulously defining permitted account types. Furthermore, it implements robust role-based access controls to precisely align access restrictions with the delineated roles and responsibilities of users. Additionally, it provides explicit guidance on remote access protocols and procedures.
3.1.3	Control the flow of CUI in accordance with approved authorizations.	The system is configured to protect DesignWorld proprietary information flow by use of VPN tunnels and a series of boundary protection devices.
3.1.4	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	DesignWorlds system is configured to use role based access controls to enforce the Principle of Least Privilege. This ensures users are given the minimum privileges to conduct this scope of work.
3.1.5	Employ the principle of least privilege, including for specific security functions and privileged accounts.	DesignWorlds system is configured to use role based access controls to enforce the Principle of Least Privilege. This ensures only certain roles can conduct security related tasks and restricts privileged accounts from being accessed by day-to-day users.

Identifier	Security Requirement	DesignWorld Implementation
3.1 Access Control		
3.1.6	Use non-privileged accounts or roles when accessing nonsecurity functions	DesignWorlds Privileged User Guide specifies when it is/when it isn't acceptable to use a privileged user account.
3.1.7	Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.	DesignWorlds system is configured to use role based access controls to enforce the Principle of Least Privilege and log the execution of privileged functions. This ensures that audit events are generated anytime a non-privileged account tried to execute a privileged function.
3.1.8	Limit unsuccessful logon attempts.	DesignWorlds system is configured to enforce a account lockout after 3 unsuccessful login attempts. The account is automatically unlocked after 15 minutes.
3.1.9	Provide privacy and security notices consistent with applicable CUI rules.	DesignWorlds system is configured to display an organizational approved System Use notification to all users accessing the network.
3.1.10	Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity	The system session is configured to lock after 15 minutes of inactivity. The session lock conceals previously visible information with an organization approved publicly viewable image.
3.1.11	Terminate (automatically) a user session after a defined condition.	The system is configured to terminate all session after 15 minutes of inactivity to reduce the risk of unauthorized access to sensitive information. Session termination mechanisms are integrated into the systems network infrastructure and applications.
3.1.12	Monitor and control remote access sessions.	The organization employs a comprehensive Remote Access Policy outlining the requirements, procedures, and responsibilities, for remote access sessions to organizational systems and resources. Additionally, DesignWorld uses robust auditing solutions, like SPLUNK, capable of logging and tracking remote access sessions in real-time.
3.1.13	Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.	DesignWorld implements a FIPS compliant VPN solution to provide secure remote access for employees working from remote locations. The VPN solution utilizes FIPS-approved cryptographic algorithms and protocols.
3.1.14	Route remote access via managed access control points.	DesignWorld utilizes a VPN gateway to facilitate secure remote access to internal network resources.

Identifier	Security Requirement	DesignWorld Implementation
3.1 Access Control		
3.1.15	Authorize remote execution of privileged commands and remote access to security-relevant information.	DesignWorlds system is configured to use role based access controls to leverage which limited scope of users are allowed to execute privileged commands remotely and access security-relevant information remotely.
3.1.16	Authorize wireless access prior to allowing such connections	DesignWorld implements usage restrictions and configurations/connection requirements for wireless access to the system in accordance wit their Wireless Access Policy.
3.1.17	Protect wireless access using authentication and encryption	DesignWorlds system is configured to utilize VPN technology to establish secure encrypted tunnels for remote access in conjunction with strong encryption standards, such as AES with 256-bit encryption, to protect data transmitted over wireless networks.
3.1.18	Control connection of mobile devices.	DesignWorld implements usage restrictions and configurations/connection requirements, and implementation guidance for organization controlled mobile devices in accordance with their Mobile Device Management Policy.
3.1.19	Encrypt CUI on mobile devices and mobile computing platforms. [23]	DesignWorld mobile devices, such as smartphones and tablets, issued to employees are configured to enable encryption for all data stored on the devices. The organization also utilizes Mobile Device Management solutions to centrally manage encryption policies, enforce encryption settings, and remotely wipe or disable devices in case of loss or theft.
3.1.20	Verify and control/limit connections to and use of external systems.	DesignWorld will develop, maintain, and store MOUs with organizations to ensure verification, configurations, and authorized use of external information systems.
3.1.21	Limit use of portable storage devices on external systems.	DesignWorld will develop, maintain, and store MOUs with organizations to ensure verification, configurations, and authorized use of external information systems.
3.1.22	Control CUI posted or processed on publicly accessible systems.	N/A. DesignWorld does not store any proprietary information on publicly accessible systems.

Identifier	Security Requirement	DesignWorld Implementation
3.2 Awareness and Training		
3.2.1	Ensure that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.	DesignWorld has an organization wide training program that requires annual employee training to include Security Awareness Training, Role-Based Security Training, and Insider Threat Training.
3.2.2	Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities.	DesignWorld has an organization wide training program that requires annual employee training to include Security Awareness Training, Role-Based Security Training, and Insider Threat Training.
3.2.3	Provide security awareness training on recognizing and reporting potential indicators of insider threat.	DesignWorld has an organization wide training program that requires annual employee training to include Security Awareness Training, Role-Based Security Training, and Insider Threat Training.

Identifier	Security Requirement	DesignWorld Implementation
3.3 Audit and Accountability		
3.3.1	Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity	DesignWorlds Audit and Accountability Policy identifies auditable events, including user logins, access attempts to sensitive data, modifications to system configurations, and security-related incidents. Logging is configured across the entire information system. The organization establishes retention policies for all audit logs to be retained for a minimum of 1 year to support monitoring, analysis, investigation, and reporting activities. The Audit and Accountability Policy will be reviewed and updated for continuity annually.
3.3.2	Ensure that the actions of individual system users can be uniquely traced to those users, so they can be held accountable for their actions.	DesignWorlds Audit and Accountability Policy identifies auditable events, including user logins, access attempts to sensitive data, modifications to system configurations, and security-related incidents. Logging is configured across the entire information system. The organization establishes retention policies for all audit logs to be retained for a minimum of 1 year to support monitoring, analysis, investigation, and reporting activities. The Audit and Accountability Policy will be reviewed and updated for continuity annually.
3.3.3	Review and update logged events.	DesignWorlds Audit and Accountability Policy identifies auditable events, including user logins, access attempts to sensitive data, modifications to system configurations, and security-related incidents. Logging is configured across the entire information system. The organization establishes retention policies for all audit logs to be retained for a minimum of 1 year to support monitoring, analysis, investigation, and reporting activities. The Audit and Accountability Policy will be reviewed and updated for continuity annually.
3.3.4	Alert in the event of an audit logging process failure.	The information system is configured to alert system administrators if an audit logging process failure error occurs. These errors include software failures, hardware failures, or audit record storage capacity being reached or exceeded.

Identifier	Security Requirement	DesignWorld Implementation
3.3 Audit and Accountability		
3.3.5	Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity.	The information system SEIM is configured to aggregate logs for comprehensive report generating across the organization to maximize analysis and investigative efforts.
3.3.6	Provide audit record reduction and report generation to support on-demand analysis and reporting.	The information system SEIM is configured to aggregate logs for comprehensive report generating across the organization to maximize analysis and investigative efforts.
3.3.7	Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records	The information system is configured to synchronize internal system clocks with an NTP server as the authoritative source when generating time stamps for audit records.
3.3.8	Protect audit information and audit logging tools from unauthorized access, modification, and deletion.	The information system is configured to only allow access to the audit logging tools and audit event information to those authorized.
3.3.9	Limit management of audit logging functionality to a subset of privileged users.	The information system is configured to only allow access to the audit logging tools and audit event information to those authorized.

Identifier	Security Requirement	DesignWorld Implementation
3.4 Configuration Management		
3.4.1	Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.	The organization maintains baseline configurations and inventories of their information systems to include hardware, software, firmware, and security configuration settings.
3.4.2	Establish and enforce security configuration settings for information technology products employed in organizational systems.	The organization maintains baseline configurations and inventories of their information systems to include hardware, software, firmware, and security configuration settings.
3.4.3	Track, review, approve or disapprove, and log changes to organizational systems.	The organization tracks, reviews, approves, disapproves, and logs changes to organizational systems in accordance with their Configuration Management Policy.
3.4.4	Analyze the security impact of changes prior to implementation.	The organization conducts a security impact analysis for the proposed changes to the information system to determine any potential security impacts before implementation.
3.4.5	Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems.	Changes to the information system are conducted by qualified and authorized individuals in accordance with the Configuration Management Policy.
3.4.6	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	The information system is configured to limit the services available to users based on the services essential to successfully perform their scope of work using the principle of least privilege.
3.4.7	Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.	The organization restricts the use of nonessential software by determining which functions, ports, protocols, and/or services need to be restricted. These identified items are reviewed annually for continuity.
3.4.8	Apply deny-by-exception (blacklisting) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software.	The system is configured to a deny by exception policy and an allow by exception policy for all unauthorized and authorized software. The list is reviewed annually.

Identifier	Security Requirement	DesignWorld Implementation
3.4 Configuration Management		
3.4.9	Control and monitor user-installed software.	N/A. Only approved privileged users can install software.

Identifier	Security Requirement	DesignWorld Implementation
3.5 Identification and Authentication		
3.5.1	Identify system users, processes acting on behalf of users, and devices.	The information system is configured so that system users and processes acting on behalf of system users or devices are positively identified. All users will require to have their identity verified before being granted access to the information system.
3.5.2	Authenticate (or verify) the identities of users, processes, or devices, as a prerequisite to allowing access to organizational systems.	The information system is configured so that system users and processes acting on behalf of system users or devices are positively identified. All users will require to have their identity verified before being granted access to the information system.
3.5.3	Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts. [24] [25].	The information system is configured to require multi factor authentications for all user accounts.
3.5.4	Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.	The information system is configured to require multi factor authentication for all user accounts.
3.5.5	Prevent reuse of identifiers for a defined period.	The organization prevents the reuse of identifiers indefinitely. This prevents any confusion should the need for an investigation arise.
3.5.6	Disable identifiers after a defined period of inactivity.	The information system is configured to automatically disable inactive identifiers after 30 days of inactivity.
3.5.7	Enforce a minimum password complexity and change of characters when new passwords are created.	The information system is configured to enforce password complexity requirements. The system will require users to change 3 characters when new passwords are created.
3.5.8	Prohibit password reuse for a specified number of generations.	The information system is configured to enforce password complexity requirements. The system will enforce a password history requirement of 12 generations.
3.5.9	Allow temporary password use for system logons with an immediate change to a permanent password.	The information system is configured to force users to change any temporary password upon initial login.
3.5.10	Store and transmit only cryptographically-protected passwords.	The information system is configured to only store and transmit hashed passwords.

Identifier	Security Requirement	DesignWorld Implementation
3.5 Identification and Authentication		
3.5.11	Obscure feedback of authentication information	The information system is configured to obscure authentication information depending on the terminal being used as the user types it.

Identifier	Security Requirement	DesignWorld Implementation
3.6 Incident Response		
3.6.1	Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.	Our system's incident response capability spans from preparation to user response, drawing from diverse data sources for swift incident management. Tailored training across roles ensures readiness, emphasizing a proactive security posture and operational resilience.
3.6.2	Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization.	Our approach to incident management involves detailed tracking, documentation, and timely reporting, ensuring compliance and enhancing our security posture through informed analysis and continuous refinement.
3.6.3	Test the organizational incident response capability.	The goal here is to set a routine timeline to measure how effective or efficient its incident response plan is by performing scheduled drills at all locations. Capability must include personnel and equipment as well as detailed strategic procedures on how to response a specific incident.

Identifier	Security Requirement	DesignWorld Implementation
3.7 Maintenance		
3.7.1	Perform maintenance on organizational systems.[26].	Scheduled and routine maintenance for all hardware and software as well as mobile device use across all locations done by a trusted third-party. This is to ensure trust in the overall system.
3.7.2	Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.	N/A
3.7.3	Ensure equipment removed for off-site maintenance is sanitized of any CUI.	N/A
3.7.4	Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems.	Design World ensures that all media across its system undergoes diagnostic tests for malicious code prior to use.
3.7.5	Require multi factor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.	N/A.
3.7.6	Supervise the maintenance activities of maintenance personnel without required access authorization.	Design World supervises maintenance activities by personnel lacking required access authorization, including vendors and consultants. Through rigorous risk assessments, we issue temporary, tightly controlled credentials, ensuring security without hindering necessary maintenance.

Identifier	Security Requirement	DesignWorld Implementation
3.8 Media Protection		
3.8.1	Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital.	Design World rigorously protects proprietary on all system media, ensuring access is strictly limited to authorized personnel. We employ physical controls, secure storage, and regular inventories to safeguard both digital and non-digital media within secure environments.
3.8.2	Limit access to CUI on system media to authorized users	At Design World, access to proprietary on system media is limited to authorized users. Through physical controls and secure storage protocols, including a media check-out system, we maintain strict control and accountability for sensitive information.
3.8.3	Sanitize or destroy system media containing CUI before disposal or release for reuse.	Design World meticulously sanitizes/destroys all system media containing proprietary before disposal or reuse, covering both digital and non-digital formats. Doing methods like clearing, purging, and destruction to ensure information cannot be recovered, adhering to standards to protect data confidentiality in line with NARA policy and SP 800-88 guidelines.
3.8.4	Mark media with necessary CUI markings and distribution limitations. [27]	N/A
3.8.5	Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.	N/A
3.8.6	Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.	N/A
3.8.7	Control the use of removable media on system components.	Enable denial (block) use any personal and/or unauthorized or unapproved media storage devices on all systems and restrict the use of media storage devices to in office provided components.

Identifier	Security Requirement	DesignWorld Implementation
3.8 Media Protection		
3.8.8	Prohibit the use of portable storage devices when such devices have no identifiable owner.	Design World enforces a policy that prohibits the use of portable storage devices without a clear, identifiable owner. This policy aims to mitigate risks by ensuring accountability and responsibility for the security of the devices, thereby reducing vulnerabilities such as the potential for malicious code insertion.
3.8.9	Protect the confidentiality of backup CUI at storage locations.	At Design World, we safeguard the confidentiality of proprietary information at all storage locations, utilizing cryptographic mechanisms or physical controls as necessary. This protection covers both system-level and user-level information, ensuring that all backed-up data remains secure and confidential.

Identifier	Security Requirement	DesignWorld Implementation
3.9 Personnel Security		
3.9.1	Screen individuals prior to authorizing access to organizational systems containing CUI.	Design World rigorously screens individuals before granting them access to organizational systems containing proprietary information. This vetting process assesses conduct, integrity, judgment, and reliability to maintain trustworthiness. Our screening activities are in line with federal standards and tailored to the access levels required for each position, ensuring the security of sensitive information.
3.9.2	Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers	The organization validates need-to-know for individuals with access to proprietary information. All access is removed immediately upon termination and re-validated upon transfer.

Identifier	Security Requirement	DesignWorld Implementation
3.10 Physical Protection		
3.10.1	Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals.	The organization has postured itself to also enforce the Principle of Least Privilege at the physical level. This ensures users are given the minimum access to complete their scope of work. These accesses are validated on an annual basis.
3.10.2	Protect and monitor the physical facility and support infrastructure for organizational systems.	The organization protects and monitors the physical facility and support infrastructure for organizational systems with badge readers and video surveillance systems.
3.10.3	Escort visitors and monitor visitor activity.	The organization leverages sign-in visitor logs and visitor badges to monitor escorted visitor activity.
3.10.4	Maintain audit logs of physical access.	The organization retains all physical copies of sign-in visitor logs for a minimum of 3 years or until digital copies of the logs are archived.
3.10.5	Control and manage physical access devices.	The organization tracks and controls all physical access devices in a Physical Access Control Log. This log annotated whether a device is currently issued out to an individual or if it is checked in.
3.10.6	Enforce safeguarding measures for CUI at alternate work sites.	N/A

Identifier	Security Requirement	DesignWorld Implementation
3.11 Risk Assessment		
3.11.1	Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI	Information system risk assessments are conducted annually or if deemed necessary. The organization will incorporate risk assessment findings into mandatory annual training.
3.11.2	Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.	At a minimum, the organization will scan for vulnerabilities twice a month. Once before system patching and again after system patching.
3.11.3	Remediate vulnerabilities in accordance with risk assessments.	The organization system administrators will remediate all vulnerabilities that patches are available for. A risk assessment and prioritization will only be conducted if the patch interrupts critical business operations.

Identifier	Security Requirement	DesignWorld Implementation
3.12 Security Assessment		
3.12.1	Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.	The organization will evaluate and validate all security controls annually.
3.12.2	Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.	The organization will develop a Plan of Action for any security requirement that cannot be met. The requirement will be tracked on the plan of action till the control in successfully met.
3.12.3	Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.	The organization will evaluate and validate all security controls annually.
3.12.4	Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems. [28]	The Information System Security Plan will be reviewed and validated annually for continuity.

Identifier	Security Requirement	DesignWorld Implementation
3.13 System and Communication Protection		
3.13.1	Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.	The DesignWorld Information system utilizes VPNs to protect information transmitted and received by organizational systems.
3.13.2	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	N/A
3.13.3	Separate user functionality from system management functionality.	The DesignWorld information system separates system and user functionality by isolating administrative interfaces on different domains and with additional access controls.
3.13.4	Prevent unauthorized and unintended information transfer via shared system resources.	The information systems access control and authentication mechanism are configured to prevent the unauthorized and unintended information transfer via shared system resources by prior users or roles.
3.13.5	Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.	N/A
3.13.6	Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).	The organizations utilize a deny all, permit by exception to ensure only the necessary network communication traffic is being allowed.
3.13.7	Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks (i.e., split tunneling).	Configuration settings will allow split tunneling but limit communication of remote devices to system resources if assigned user is not physically present on site.

Identifier	Security Requirement	DesignWorld Implementation
3.13 System and Communication Protection		
3.13.8	Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.	Design World employes Cryptography to support a variety of its defined security solutions such as the protection of proprietary data and/pr information, the provision and implementation of digital signatures, and the enforcement of information separation when authorized individuals and/or third-parity partners with the necessary clearances but lacking the necessary formal access approvals. Notably the use of applicable cryptographic standards such as FIPS-validated cryptography and NSA-approved cryptography.
3.13.9	Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.	Design world is designed to enhance security by automatically terminating network connections at the end of communication sessions or after a specified period of inactivity. This applies to both internal and external networks, ensuring that TCP/IP addresses or port pairs, as well as application-level networking assignments, are promptly de-allocated. By setting inactivity timeouts, we maintain a balance between operational efficiency and security, minimizing potential vulnerabilities associated with idle connections.
3.13.10	Establish and manage cryptographic keys for cryptography employed in organizational systems.	N/A
3.13.11	Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.	Design World employes Cryptography to support a variety of its defined security solutions such as the protection of proprietary data and/pr information, the provision and implementation of digital signatures, and the enforcement of information separation when authorized individuals and/or third-parity partners with the necessary clearances but lacking the necessary formal access approvals. Notably the use of applicable cryptographic standards such as FIPS-validated cryptography and NSA-approved cryptography.

Identifier	Security Requirement	DesignWorld Implementation
3.13 System and Communication Protection		
3.13.12	Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.[29].	Design World makes use of collaborative computing devices throughout its entire network to improve both logical and physical security. Such devices as cameras, microphones and other signal applications should themselves be protected by firewall and cryptography to secure data collected from being hacked or from remote takeover by hackers.
3.13.13	Control and monitor the use of mobile code.	N/A
3.13.14	Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.	Design World network architecture set-up is aimed at separating voice and data on logically different networks and subnets with separate RFC 1918 address blocks should be used for voice and data traffic, with separate DHCP servers for each. Also the employment of intrusion detection and VOIP firewall protection at the voice gateway while using strong authentication andaccess control on the voice gateway system and a stateful packet filters and IPsec or Secure Shell (SSH) for all remote management and auditing access.
3.13.15	Protect the authenticity of communications sessions.	Design World employs the use of AES level cryptography to protect all data and information at every level of function or use, including proprietary information. *Design World maintains continuous monitoring as a means of achieving this implementation.
3.13.16	Protect the confidentiality of CUI at rest.	Design World employs the use of AES level cryptography to protect all data and information at every level of function or use, including proprietary information. *Design World maintains continuous monitoring as a means of achieving this implementation.

Identifier	Security Requirement	DesignWorld Implementation
3.14 System and Information Integrity		
3.14.1	Identify, report, and correct system flaws in a timely manner.	Design World's systems is set to determine if system components (Functional and Non-functional) have applicable security-relevant software and firmware updates installed regularly and reviewed by systems admin to minimize flaws.
3.14.2	Provide protection from malicious code at designated locations within organizational systems.	Design World systems implement both signatures based; non-signature based malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code and set to automatically update malicious code protection mechanisms as new releases are available in accordance with organizational configuration management policy and procedures. Also employ malicious code configuration protection mechanism to scan and block any unauthorized codes.
3.14.3	Monitor system security alerts and advisories and take action in response.	N/A
3.14.4	Update malicious code protection mechanisms when new releases are available.	Design World systems implement both signature based; non-signature based malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code and set to automatically update malicious code protection mechanisms as new releases are available in accordance with organizational configuration management policy and procedures. Also employ malicious code configuration protection mechanism to scan and block any unauthorized codes.
3.14.5	Perform periodic scans of organizational systems and real-time scans of files from external sources as files are downloaded, opened, or executed.	Design World ensures the integrity of systems across its network by performing regularly scheduled real-time scans of all external sources, files, downloads, and attachable devices.

Identifier	Security Requirement	DesignWorld Implementation
3.14 System and Information Integrity		
3.14.6	Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.	Design World sets criteria for unusual or unauthorized activities or conditions for inbound and outbound communications traffic by monitoring all inbound and outbound communications traffic by way of an IDS/IPS automated and/or real-time system monitoring. Also, Design World implements encryption to all internal and external communication to safeguard private data and system integrity.
3.14.7	Identify unauthorized use of organizational systems.	The organization will monitor and detect unauthorized use of the organizational systems using tools like Splunk, and other network monitoring software.

4. RECORD OF CHANGES

Date	Description	Made By:
3/15/2024	Initial Submission	Team Member
3/15/2024	Added Section 1	Team Member
3/16/2024	Added Requirements to Section 3	Team Member
3/19/2024	Added Network Topology to section 2	Team Member
3/20/2024	Added Requirements to Section 3	Allison
3/20/2024	Submitted for Approval	Team Member

5. APPROVALS

The team responsible for carrying out this penetration test is represented in the table below. Penetration testing shall only proceed following authorization by Design World.

5.1 Author

Role	Printed Name	Signature	Date
Project Manager	[Team Member]	[Team Member]	20 Mar 2024
Lead Penetration Tester	[Team Member]	[Team Member]	20 Mar 2024
Lead Compliance and Governance Expert	[Team Member]	[Team Member]	20 Mar 2024
Lead Security Architect	[Team Member]	[Team Member]	20 Mar 2024
Lead Incident Responder	Allison Manning	[signature on file]	20 Mar 2024

5.2 Client

Company	Role	Printed Name	Signature	Date
USD Cyber Cloud	Chief Technical Officer			
Design World	Chief Executive Officer			
Design World	Director, IT			

6. GLOSSARY OF TERMS

Term	Definition
AES	Advanced Encryption Standard
CUI	Controlled Unclassified Information
DC	Domain Controller
DHCP	Dynamic Host Configuration Protocol
FIPS	Federal Information Processing Standards
FS	File Server
IDS/IPS	Intrusion Detection System/Intrusion Prevention System
IPsec	Internet Protocol Security
ISSP	Information System Security Plan
NIST	National Institute of Standards and Technology
NTP	Network Time Protocol
SSH	Secure Shell
SPLUNK	Software used for searching, monitoring, and analyzing machine-generated data via a Web-style interface
VPN	Virtual Private Network
VoIP	Voice over Internet Protocol

7. DOCUMENT REFERENCE TABLE

DOC ID	TITLE	VERSION
1	Design World Statement of Work (SOW)	1
2	Design World Case Study Requirements	1
3	**A**3C001 - System Security Requirements for Design World	2
4	**A**3C002 - Vulnerability Assessment Plan	1
5	**A**3C003 - Vulnerability Assessment Report	1
6	**A**3C004 – Penetration Test Plan	1
7	**A**3C005 – Penetration Test Report	1
8	**A**3C006 – Hardening Plan	1
9	**A**3C007 – Security Hardening Report	1
10	**A**3C008 - Final Penetration Test Report	1
RFI-001-**A**3C	Client Discussion Forum - Security Objectives	[Team Member] Jan 11 7:40pm
RFI-002-**A**3C	Client Discussion Forum - Security Objectives	[Team Member] Jan 20 3:32pm
RFI-003-**A**3C	Client Discussion Forum - Security Objectives	[Team Member] Jan 20 4:01pm
RFI-004-**A**3C	Clent Discussion Forum - Password Verification	[Team Member] Jan 26 6:11 pm

8. REFERENCES

Allen, J. (2022, December 15). *What should a data security policy include? (W/ Sample template)*. PurpleSec. Retrieved March 18, 2024, from https://purplesec.us/learn/data-security-policy/

BenQ. (n.d.). What is CVE and CVSS. Retrieved January 22, 2024, from https://www.benq.com/en-hk/business/resource/trends/what-is-cve-and-cvss.html

CIS CentOS Linux 7 Benchmark. (2023, December 22). CIS. Retrieved January 17, 2024, from https://www.cisecurity.org/cis-benchmark

CIS Microsoft Windows Server 2016 Benchmark. (2023, April 14). CIS. Retrieved January 17, 2024, from https://www.cisecurity.org/cis-benchmarks

CIS Microsoft Windows Server 2016 STIG Benchmark. (2023, October 20). CIS. Retrieved January 17, 2024, from https://www.cisecurity.org/cis-benchmark

CIS Ubuntu Linux 20.04 LTS STIG Benchmark. (2023, August 31). Retrieved January 17, 2024, from https://www.cisecurity.org/cis-benchmarks

CIS Ubuntu Linux 20.04 LTS Benchmark. (2023, June 29). Retrieved January 17, 2024, from https://www.cisecurity.org/cis-benchmarks

CIS Microsoft Windows 10 Enterprise Benchmark. (2023, March 7). Retrieved January 17, 2024, from https://www.cisecurity.org/cis-benchmarks

Common Vulnerability Scoring System SIG. (n.d.). Retrieved January 19, 2024, from https://www.first.org/cvss/

Derbentseva, N., & Träber-Burdin, S. (2020). Chapter 5 – CYBER SECURITY: AN ORGANIZATIONAL PERSPECTIVE. In *Human Systems Integration Approach to*

Cyber Security (STO Technical Report, Vol. TR-HFM-259, pp. 5–1). North Atlantic Treaty Organization and Science & Technology Organization. Retrieved March 9, 2024, from https://www.sto.nato.int/publications

Dinges, B. (2002, August 1). A Certification and Accreditation Plan for Information Systems Security programs (Evaluating the Effectiveness of an Information Systems Security Program). *SANS Institute*. Retrieved March 10, 2024, from https://sansorg.egnyte.com

Grassi, P., Fenton, J., Newton, E., Perlner, R., Regenscheid, A., Burr, W., & Richer, J. (2020, March). NIST Special Publication 800-63B. *NIST*. NIST. Retrieved March 10, 2024, from https://doi.org/10.6028/NIST.SP.800-63b

HackTricks. (2023). Web API Pentesting. Retrieved February 18, 2024, from https://book.hacktricks.xyz/pentesting-web/api-pentesting

Information Security Policy Templates | SANS Institute. (n.d.). Retrieved March 18, 2024, from https://www.sans.org/information-security-policy/

Joint Task Force. (2020). Security and Privacy Controls for Information Systems and Organizations. In *NIST* (Special Publication 800-53 Rev. 5). NIST. https://doi.org/10.6028/NIST.SP.800-53r5

Ross, R., Pillitter, V., Dempsey, K., Riddle, M., & Guissanie, G. (2021). Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations. In *NIST* (Special Publication 800-171). NIST. https://doi.org/10.6028/NIST.SP.800-171r2

Swanson, M., Hash, J., & Bowen, P. (2006, February). *Guide for developing Security Plans for Federal Information Systems* (NIST Special Publication 800-18). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-18r1

Triaxiom Security. (2023). Our API Penetration Testing Methodology. Retrieved February 18, 2024, from https://www.triaxiomsecurity.com/api-penetration-test-methodology

Qualysec. (2023). API Penetration Testing A Complete guide 2023. Retrieved February 20, 2024, from https://qualysec.com/api-penetration-testing/