Visualware®
Network Measurement and Quality Assessment

RISK MITIGATION PROCEDURES

The purpose of this document is to provide a clear statement of the procedures that the Company undertakes to underwrite day-to-day business operations.

This document outlines the daily, weekly, and monthly tasks that the Company undertakes to identify potential risk incidents and, where possible, the process to mitigate or limit such risks.

Revisions:

Date	version	Summary
3/12/2023	1.1	Procedural changes for asset retention
4/1/2023	1.2	Change to information retention, additions for audit procedures. Hard drive encryption adopted, pending approval
5/22/2023	1.3	Effective June 5, 2023 all computer devices requesting network connection approval or requested for audit approval will be required to have approved hard drive and USB encryption permanently enabled. UTCS02 approval excluded.
03/15/24	1.4	AHA category changed acronym ASA to conform to V12 documentation.

1.0 Information Assets

1.1 Information Asset Grades

Change Notice 1.2. Effective April 1, 2023, with the exception of email, all information entrusted to any Company employee, in the course of undertaking Company business, that originates from a source outside the Company, regardless of form e.g., paper or digital, must be graded under one of the four classifications documented in this section:

Public

Public information assets are defined as data that is freely available for access by any person regardless of whether the person works for the organization or is an individual providing the information. For example, public web sites, publicity campaigns, media information published for public consumption such as a press release etc.

Internal use

Internal use data assets are defined as information that is released, to the Company or by the Company, in the course of conducting its business. Such information is to be used only for internal purposes and must not be provided to any person(s) not directly employed by the Company. For example, this may include support data provided for a technical support ticket, email exchanged information, shared online meeting information or internal Company information provided to employees for the purpose of conducting business.

Confidential

In confidence information assets are defined as information that is provided, to the Company or by the Company, in the course of conducting its business, where the audience is intentionally limited because of confidentiality concerns, essentially a secret that is provided on a need-to-know basis. For example, information from a private desktop computer, financial information that is presented in a meeting for only those attending the meeting. Information provided under the umbrella and expectation of an NDA.

Restricted/Highly Sensitive

Information assets provided to a select Company audience and the information provided is strictly under the terms of ‘professional trust’ then such information must not be given to any persons outside that of audience unless authorized in writing by the information owner. If the person providing this sensitive information is not the information owner, then the information should be declined. For example, Security credentials to access a private computer or application, cyber encryption keys, strategic business information that would be valuable to a competitor, internal company financials, sensitive employment or personnel information.

1.4 Email Information Assets

Email services will routinely, directly or indirectly, contain information that originates from outside the Company. Effective May 14, 2023, all company computer devices, including mobile devices, submitted to Sysadmin for network access approval will be required to have local data encryption enabled by default. After May 14, 2023 no computer device will be approved access to any Company network subnet unless local data encryption is enabled.

1.2 Digital Information Asset Retention

With the exception of email, all digital information asset retention periods logged into a Company data repository will inherit the following maximum retention periods.

Public	**no limit.**
Internal use	**360 days**
Confidential	**90 days.**
Highly sensitive	**30 days.**

1.3 Non-Digital Information Assets

To comply with section 1.2 any information assets provided as documents must be converted and stored in digital form. If documents are also required to be retained in the original form, then they must be clearly marked with the information grade and the acceptance date before the documents are submitted to line management for secure filing, otherwise documents must be returned to the information owner.

1.4 Information Asset Auditing

Information assets will be reviewed weekly by System Administration.

If information assets are found to be incorrectly graded, including the retention period, an ‘information’ violation IR will be escalated to the line manager for review.

All information assets marked to expire, that are still required for the intended purpose, for which the information was provided, for example a support ticket that remains open, then a retention extension approval must be provided in writing prior to the retention deadline.

All information assets that exceed the allocated retention period will be deleted without further reference.

2.0 Computer Device

This section documents the procedures that are mandated to approve Company and personal computer devices that require or request a connection to a Company subnet for which it is not approved. These procedures are designed to ensure that all devices conform to the Company requirements for information confidentiality, Information retention, cyber threat mitigation and other ethical standards.

2.1.1 All computer devices must be inspected and granted approval by System Administration before connecting or attempting to connect a computer device to any Company network service.

2.1.2 If any device connects, or attempts to connect, to a Company subnet that has no active approval status or the approval status has expired a ‘connect’ violation IR will be escalated to the line manager for review.

2.1.3 For continuity of network access connection approvals must be submitted for renewal at least 2 working days before the current approval period expires. Note, if any device is connected at the time approval expires, regardless of whether the connected device is actively in use or not, a ‘connect’ violation IR will be escalated to the line manager for review.

2.1.4 Any computer device requested or submitted for a sysadmin audit, regardless of approval status, must not connect, attempt to connect, or remain connected to a Company subnet until audit approval is granted.

2.1.5 Any computer device, under ‘audit’ that is found to have (or has had in the past) violated any of the Company security policies, connection policies, information confidentiality policies or ethics policies, will automatically be denied approval and an ‘audit’ violation IR will be escalated to line management for review.

2.1.6 Any computer device configuration that is denied approval as a result of a configuration change since the prior audit, then the computer device configuration will be automatically updated to conform and a configuration violation IR will be escalated to line management for review.

2.1.7 Computer devices found to have (or has had in the past) unapproved applications installed, including applications that have been identified as removed, that are not documented for the device, a configuration violation IR will be escalated to line management for review.

2.1.8 Connection approval is automatically voided if a device connects or attempts to connect to an unapproved Company connection. A connect violation IR will be escalated to the line manager for review.

2.2 Audit Process Summary

The following section outlines the scope of the device audit test process.

The purpose of the audit is to verify that a device under test (DUT) conforms to the configuration and policy requirements for Company network access. The audit process, includes but is not limited to:

1. Hardware and configuration changes
2. User role access and credentials for access
3. User accounts
4. Operating system (OS) and version and files
5. Event audit logs
6. Mandated/Restricted applications
7. Malware, Spyware, Antivirus status and history
8. Browser history, activity logs, content, and cached files
9. Email history, inbox recipients, outbox recipients sent/received, and contacts
10. Information, grade and retention
11. Network adapters, configuration, MAC address, gateway, DNS, and subnet
12. Present files, executables, and all other content types
13. Removed files, executables, and all other content types
14. Hard drive
15. USB and hard drive encryption (UTCS02 excluded)
16. Drivers and versions
17. System registry

Notes: The Company device audit process examines all content on the hard drive which includes access to private information assets on personal devices. All audit scan results are kept for future audit baseline comparisons.

2.2.1 Approval Certifications

System Administration issues an approval code when a DUT is passed. The following define the five certification approvals:

- UPCS01 - Production Customer Cloud
  Provides access to USA Cloud services
  Seattle, Los Angeles, Denver, Chicago, New York, Washington DC, and Miami.

- IPCS02 - International Customer Cloud
  Provides access to International Cloud services
  London, Paris, Tokyo, Seattle, and Sydney.

- UDCS01 - Development Cloud
  Provides access to Cloud development services
  London, Houston, and San Jose.

- UTCS01 - Test Services
  Provides access to Lab Test services
  London and Houston.

- UTCS02 - Release Test Services
  Eligible for access to RC & GA Test sessions.
  All devices UTCS02 on request.

With the exception of UTCS02 all connection certification approvals are limited to max 30 days. UTCS02 approvals for RC and GA testing only.

3.0 RISK MITIGATION PROCEDURES

This section documents the processes and tasks that are undertaken by the Company to proactively underwrite the integrity of business operations on a day-to-day basis. The purpose and intent of these processes is to capture, expose, and mitigate risk events that can affect the Company's ability to conduct its business.

Some mitigation processes are automated to minimize human errors associated with daily repetitive tasks. However, other processes are specifically implemented as manual processes to ensure all information processed is disseminated correctly. This approach maximizes human resources and fosters a culture of knowledge, responsibility, and accountability across the business teams.

3.1 Ingress Daily Procedures

This section covers all inbound network transactions for all Company network subnets. Approximately 80% of all ingress traffic is Application Cloud Services (**ACS**), the remaining 20% is public information services. With the exception of penetration and platform conformance, testing development and test labs excluded.

3.1.1 Ingress Cloud Service Auditing

The Company ACS production network supports all customers and each customer is managed in accordance with the Customer Service Contract.

Auditing of Cloud ingress traffic is a fully automated process that identifies and captures all service events by IP address. This IP information is one of the prime sources of the data that is reviewed daily and used to administer the network policies.

The **Cloud Services Framework** (CSF) automatically identifies all illegal ingress traffic in real-time. Additionally, the **ACS** synchronizes seven real-time system/application ingress event types to compile an audit dataset of events that is correlated to expose customer intrusion threats. The application event audit datasets are reviewed for all customer services independently and a customer violation incident report (IR) is compiled to document all identified threats as follows:

Ingress - Application Security Audit (ASA):

> Automatically generated in real-time by the CSF. All ingress transactions are (stateful) examined for transaction integrity, this includes but is not limited to, size conformance, transaction structure conformance, protocol conformance including RFC conformance, subnet access policies, illegal content policies, profile content, user permissions, user roles, and active sessions.
>
> The ASA records: ***IP, UTC, transaction type, violation rule, ISP and the full offending ingress dataset content***

Actions Taken: Where the ingress content cannot be excluded as a 'human error' event:

1. All IP addresses that identify as public user access (i.e., no user credentials required) are extracted and a security violation IR is escalated to system administration to update border policies. Additionally, ISP confirmation and ISP AUP abuse reporting is actioned for each ISP identified. Finally, all line managers are notified for information and comment.

2. All IP addresses, that identify as customer access (i.e., customer credentials), are extracted and a customer violation IR is escalated to the support line manager, account manager, and system administration for review and notification to the customer as necessary.

3. All IP addresses that identify as a Company authorized user, (i.e., a Company user profile) the offending IP information is extracted and an internal security violation IR is escalated to the user line manager as well as System Administration for investigation.

4. If the audited content URL is identified as an already known threat, an IR report is escalated to all Company staff as a red-alert for immediate comment.

Ingress - Application Traffic Audit (ATA):

Automatically generated in real-time by the CSF. This audit comprises of all ingress transactions that successfully passed the ASA audit process and are logged in the ATA. The ATA IP addresses are cross referenced to the ASA IP addresses to identify if there have been any potential customer incursions from the same IP or IP subnet.

The ATA records: ***IP, UTC, transaction type, full ingress content, the actual service response and the service result code***

Actions Taken: Where the ingress content cannot be identified as a 'human error' event:

- All IP addresses escalated from the ASA are cross-referenced to the ATA. If any IP addresses are matched a security violation IR is escalated to the customer support line manager containing all ATA/ASA identified matching IP transactions for investigation and customer notification as required.

Ingress - Application User Activity Audit (UAA):

Automatically generated in real-time by the CSF. All ingress transactions that successfully pass the ASA audit process, that then amend or change any details or privileges relating to a user identity (including administrator role), are logged in the UAA. The UAA is cross referenced to the ASA IP addresses to identify if user credentials have been compromised by an IP known for previous violations.

The UAA records: ***IP, UTC, user name, user roles, account id, Full ingress user activity Content, ISP***

Actions Taken: Where the ingress content cannot be identified as a 'human error' event:

All IP addresses from the ASA are cross-referenced to UAA. If any IP addresses are matched a credentials violation IR is escalated to the customer support line manager and System Administration for investigation and border policy changes as required.

Ingress Publish Activity Audit (PAA):

Automatically generated in real-time by the Internet Cloud Service Application.

Actions Taken: None. The Publish Activity Audit dataset is provided for engineering support only and has no requirement or benefit for correlation of ASA transactions.

Ingress System Activity Audit (SAA):

Automatically generated in real-time by the Cloud Application Service. All ingress transactions that trigger a system event are logged in one of three SAA datasets. SAA datasets contain no reference to IP assets and the ASA IP addresses are cross referenced chronologically using the UTC timestamp down to millisecond. This identifies suspect correlation events that may have affected the system processing logic, the service database(s) drivers or the memory/threading utilization limits.

The SAA profiles the following for problem detection at the system level:

UTC, [System event content dataset, records all system events of note],
[SQL DB content dataset, records all database update events],
[Memory/Thread dataset, records memory/concurrency violations]

Actions Taken: Where the ingress content cannot be identified as a 'human error' event:

- All IP addresses from the ASA are crossed referenced by the UTC timestamp. If a close match is found that correlates to any system event a system violation IR is escalated to the development line manager and engineering support line manager for investigation and further action as required. These events are not common.

3.1.2 Ingress Border Gateway Auditing

Auditing of ingress traffic for border services falls under third-party commercial applications, for example the Company web servers use Apache. Third-party applications audit all ingress traffic as a common inclusive rule base unlike the CSF which is context sensitive. The audit validation process reviews all ingress IP assets in addition to the URL content information recorded in the audit dataset.

In summary, the border ingress audit datasets are retained and reviewed on a daily basis. The **CSF** ATA audit dataset (known valid transactions) is cross referenced by IP to the border audit datasets and all unmatched IP records are retained for illegal traffic analysis as follows:

Ingress – Border Gateway Audit (BGA):

All ingress Cloud service ASA IP addresses captured as part of 3.1.1 are cross referenced to the border audit to extract all unmatched transactions for further review.

Actions Taken: For all border ingress audit datasets:

- All IP addresses escalated from the ASA are cross-referenced to the BGA dataset and all unmatched IP addresses in the BGA are retained to create a new (temporary) risk focused audit dataset.
- The ASA dataset URL content is cross referenced to the risk dataset and a list of unique IP addresses is compiled for content that matches the known ASA events.
- A security violation IR of the offending IPs is escalated to System Administration for review, border policy updates and escalation to business line managers as required.

3.1.3 Egress Border Gateway Auditing MAC, DHCP

Auditing of egress traffic at the gateway PoPs creates a dataset of all responses to ingress requests as well as originating egress requests. The egress dataset is used to validate Company policies to isolate and report:

1. Network assets accessed by unapproved devices
2. Network assets accessed from an unapproved connection
3. Application assets accessed from an unexpected device

In summary, border egress audit datasets are retained and reviewed on a daily basis to identify potential Company policy violations as follows:

Egress – Border Process:

All egress border datasets are scanned daily by the Company System Administrators using a compiled dataset of key/value rules to cross reference and automate the selection of possible Company policy violations based on rule matches as follows:

Actions Taken: Border egress audit datasets will be processed and cross-referenced as follows:

- **Domain names.** IP lookup for unapproved domain names
- **ISP.** History validation
- **IP Subnet.** Identify ISP subnets (class A – C, CIDR restrictions)
- **MAC address.** Local connect requests
- **Abnormal behavior.** This includes but is not limited to, clock time, traffic volume, transaction type, application errors.
- **Geolocation.**.
- A connect violation IR, for risk assessed IP addresses is escalated to the appropriate line managers and also to System Administration for investigation, policy changes and ISP or internal abuse reporting if required.

3.2 Application and Business Service Procedures

This section documents Company daily, weekly, and monthly application services and business services procedures. These procedures document the day-to-day processes that underwrite the delivery of the Company customer cloud, development, and technical support services.

3.2.1 Customer Cloud Services RPO/RTO

Definitions:

Recovery Point Objective (RPO) – defines the maximum amount of data (measured in time) that is allowed to be lost by the CSC.

Recovery Time Objective (RTO) – defines the maximum amount of time allowed to reestablish service in the event of a service recovery request

The Company Cloud Services production network supports all customers and each customer is managed in accordance with a Customer Service Contract (CSC).

RTO available services: 2, 4, and 8 hours

RPO available services: 1, 7, and 28 days

The CSC defines the requirement for a customer RPO and RTO.

3.2.2 Customer Cloud Services for RPO

Customer cloud applications are automatically archived (G, F, S) for recovery as follows.

RPO-1 The customer cloud service is archived **daily** in three parts.

Part 1 archive at service location to enable fast local recovery

Part 2 archive to secure SVN repository (geolocation)

Part 3 hot-standby backup to a remote location (mandated for an RPO-1 CSC)

Additional archives as specified by the CSC.

RPO-7 The customer cloud service is archived every **Sunday** in two parts.

Part 1 archive at service location to enable fast local recovery

Part 2 archive to secure SVN repository (geolocation)

Additional archives as specified by CSC

hot-standby backup to a remote location (mandated for an RTO-2 CSC)

RPO-28 The customer cloud service is archived every 4th **Sunday** in two parts.

Part 1 archive at service location to enable fast local recovery

Part 2 archive to a secure remote SVN repository (geolocation)

Additional archives as specified by CSC

hot-standby backup to a remote location (required CSC with RTO-2)

3.2.3 Customer Cloud Services for RTO

Customer cloud applications are automatically archived for recovery as follows.

RTO-2 The customer cloud service is archived based on the RPO.

hot-standby backup to a remote location mandated in CSC.

RTO-4 & 8 The customer cloud service is archived based on the RPO.

hot-standby backup to a remote location optional in CSC.

3.2.4 Customer Cloud RTO Testing

Customer cloud applications are tested for conformance to the CSC as follows.

RTO-2

The CSC hot-standby service is monitored by keep-alive every 10 minutes and an alert is escalated to operations for 3 consecutive no response events.

RTO-2, 4 & 8

All customer cloud services are recovered from the remote archive location every 2 weeks. If the RTO is exceeded by more than 10% or the RPO is exceeded by more 10% then an Incident Report (IR) is raised and sent to the relevant customer account manager and the customer support line manager.

3.3 Customer Cloud asset and services validation

This section documents Company daily, weekly, and monthly procedures, conducted by Sysadmin, to validate physical platform assets to ensure that infrastructure and services are healthy and operating within expectation.

Cloud asset validation encompasses the following:

1. Hard drive health and available space/space-delta (weekly)
2. Raid Statistics (on a server boot)
3. Processor, I/O and memory utilization (weekly)
4. Software asset versions (weekly)
5. Anti-virus and malware versions (daily)
6. Anti-virus and malware activity logs (daily)
7. Platform system and event audit logs (daily)
8. Environmental (on site quarterly)
9. Network traffic statistics delta (monthly, actioned by accounts)
10. Hard drive (quarterly)
11. Network availability and performance (10min, keep alive)
12. Redundancy (quarterly)

A system event IR is created for any non-normal (as in delta valuations) results.

4.0 INCIDENT REPORTING (IR)

This section summarizes the Company review and escalation procedures for the different IR categories documented in section 3.

4.1 IR Violation Classes

The following define the common business IR violation categories.

- Security - Ingress threat to the network that was service blocked
- Security Internal - Ingress threat to the network from a known user profile
- System - Ingress threat that correlates to a system event problem
- Customer - Ingress threat to, or from, a specific customer service
- Credentials - Ingress user profile threat that matches a penetration event
- Configuration - Sys-admin device audit fail
- Connect - Sys-admin unapproved ingress/egress connection
- Information - Sys-admin notifications and Company change notices

4.2 Incident Grading

Every violation IR is assigned a numeric classification grade from 0 (zero) to 5 (five). The grade classes, response time, and escalation points are itemized below. Any IR can be graded higher or lower based on the assessment at the time the IR is created. Additionally, line managers and system administration can change an IR grade/priority.

Grade	Type/Time(hrs)		Escalation requirements
0	Administration/NA	-	All staff required ALL policy changes and notices.
1	Ingress security/24	-	Sysadmin, customer account manager Border policies, ISP abuse report
2	Information breach/24 System event/48	-	Target customer account line manager Development line manager Engineering line manager
3	Network connect/4 Device audit//4	-	Sysadmin, employee(s) line manager Border polices
4	Customer impact/4	-	Customer account line manager Customer representative (if required) Border policies, ISP abuse report
5	Credentials/2 Security Internal /2	-	Sysadmin, all line managers Border policies

4.3 Incident Mitigation

The following section documents an outline of the procedures for managing all IR submissions. Every IR raised by any team member is sent to the attention of System Administration at incident@visualware.com.

System Administrators ensure that all IR events are validated and investigated based on the context and priority grade of the IR event and a customer support ticket if attached.

As part of the review and escalation process, system administrators distribute and gather input from all Company business teams including customer support, line management, development, engineering, accounts, sales, legal, and executive. Additionally, System Administration is responsible for SLA response times.

The following IR events are automatically escalated for review at the bi-monthly team line manager meeting, in no particular order:

1. Open for more than 7 business days
2. Grades 3, 4, or 5
3. Any ingress event that exceeds 10 from any one subnet in 24 hours
4. A network ingress event classed as ‘known’ directed/received from customer service
5. Nonpublic information leak or policy breach
6. Device audit fail
7. Any security violation identified as Internal
8. Priority 1 customer support ticket
9. Customer with 4+ open support tickets grade 2 or 3
10. CSC conformance failure for RTO/RPO
11. New customer deployment certification and approval notices
12. All Company policy updates and change notices

Additionally, any IR can be escalated for review at the bi-monthly team line manager meeting on request from:

1. Team line manager
2. Executive
3. Legal

5.0 Penetration and Conformance Testing

The Company delivers a bespoke customer Application Cloud Service in addition to standard publicly accessible WWW information services, file upload/download services, and SMTP services. Additionally, there are a number of Company internal applications such as development IDE services, repository services, license protection services, and ecommerce services.

This section documents the Company penetration and conformance procedures for application services.

The purpose of the Company penetration and conformance testing processes serves to identify and expose any threats, or potential threats, in the delivery framework of application services that could allow any person to gain access to any application service or system service, and any information contained therein, without the use of application security credentials, regardless of whether such information is sensitive or not.

Application penetration testing is conducted as part of:

1. ACS release cycles targeted for Release Candidate (RC) certification
2. ACS release cycles targeted for General Availability (GA) certification
3. Periodic Company network and public application services testing, including ACS
4. Yearly/Monthly independent outsourced ISO27000 / ISO27001 for accreditation

5.1 Periodic Penetration Test

The periodic penetration testing is conducted on a random basis 2 or 3 times a year and targets any of the Company assets that are visible on the internet including but not limited to the WWW, email, DNS, ACS, file (upload & download) and operating access services.

5.2 Release Penetration Test

ACS release testing for General Availability (GA) or Release Candidate (RC) certification incorporates penetration testing as the final test phase of the product release cycle. RC and GA certification testing is only conducted on an isolated private network. There are no restrictions on client digital assets configurations used for release testing.

5.3 Independent Penetration Test

Independent penetration testing is conduct without any Company involvement in the process or the content of the process. A Certification certificate is issued on a test pass. Certification failure allows 30 days to address and correct reported issues. Post failure, testing is conducted on a monthly basis required for 12 (pass) consecutive months.

5.4 Penetration Test Elements

The penetration test categories include, but are not limited to, the following (in no particular order):

Buffer exclusions. All ingress buffers are validated automatically on size as related to content and the application. Buffer testing specifically transmits content that exceeds normal values, small and large, for acceptance. **Failure immediate:** if any invalid ingress buffer is approved.

Volume. Ingress transactions are validated to certify conformance to acceptable stress limits. **Failure immediate:** if the test fails prior to reaching expected limits.

Illegal HTTP(s) Transaction Methods. All transaction methods are tested for acceptable use, this includes but is not limited to HEAD, DELETE, CONNECT, and PATCH. **Failure immediate:** if any one invalid transaction method is not blocked.

Cross Site Forgery (CSF). CSF is an option in the Company Application Service Cloud. This is enabled on the security settings page. When enabled any ingress URL request where the referrer for the resource requested is not the originating application service a CSF rejection is issued. **Failure:** if a known indirect referrer is not detected, stopped, and reported.

Code Injection

> **Simple (SCI).** All transactions are subject to CI detection on all request and content buffers. All transactions that are valid to the point of the injection test are tested for illegal content. **Failure immediate:** if any one defined illegal asset is passed.
>
> **Complex Code Injection (CCI).** All transactions are subject to CCI detection on request and content buffers. All transactions test for code injection that cannot be detected because the syntax is encoded or the syntax segmented into multiple safe assets which fail when combined. **Failure immediate:** if any one illegal string is not detected.

SQL Injection (SQI). All Cloud Application Service SQL APIs are subject to SQLI detection. Note, SQL API services are intentionally not natively supported by ACS. SQL is only provided to support custom externalization for use within the customer domain. **Failure immediate:** if any SQL injection event is approved.

XM/SOAP External API (XSE). XML/SOAP security option in the Company Application Service Cloud is enabled on the security settings page. When the 'Secure Mode for XML' is enabled all XML API requests are subject to four additional security policies. 1. XML restricted to permitted domains, 2. Secure parsing, 3. Parsing depth limits. 4. Recipient Checksum. **Failure immediate:** if any one XML security policy is not enforced.

Credential Policies

Content Conformance. All credential submissions are subject to conformance tests for life-cycle, repetition of use, content policy and content length. **Failure immediate:** if any credential challenge fails any content policy.

Policy Roles. All roles allocated to credentials are subject to conformance tests for privilege enforcement, public privilege inheritance, and role restrictions. **Failure immediate:** if any absent role category challenge is approved.

Public Role. Because of inheritance rules the roles allocated to public are subject to tests for acceptable use. **Failure immediate:** if any public restricted role category is approved for public.

Time To Live (TTL). All in-use credentials are subject to TTL conformance tests for, 1. Expired idle TTL, 2, Expired max-limit, 3. Combined idle max-limit. **Failure immediate:** if TTL reaches/exceeds a defined limit.

Activity Auditing All in-use credentials audit major user events, this includes but is not limited to, log-in, log-out, modification of credential policies and modification of administration assets. **Failure immediate:** if any mandated audit event is not reported

Access Control

Subnet and IP Restrictions (SR). All ingress transactions are tested for SR restrictions. **Failure immediate:** if any IP, IP range or IP/CIDR challenge is granted access.

Application URL restrictions (AUR). Ingress application URL policy restrictions. **Failure immediate:** if any blocked application URL challenge is granted access.

User Role Change (URC. Application access user role changed by subnet. **Failure immediate:** if any URL permissions change by subnet fails to be enforced.

Domain Host Restriction (DHR). All ingress transactions are subject to the defined DHR domain name or IP address restrictions for HTTP and HTTPs codebase constructs. **Failure immediate:** if any ingress HTTP(s) URL request is able to access application services using an unauthorized domain or IP.

Secure Cookie Options (SCO). SCO is an option in the Company Cloud Application Services on the security settings page. The two selection options enable ‘Secure Cookies’ and ‘HTTP Only’. **Failure Immediate:** if any request fails to block a secure cookie by HTTP or HTTP Only cookie not by HTTP.

File Access Requests. Company Cloud Application Services automatically implements a number of restrictions for file access requests. Ingress recursive requests, relative file title requests, root request, and encoded requests are prohibited. **Failure Immediate:** if any file request is granted that is prohibited by content type, by access type, by permitted name, by location, or by permissions.

Predictable Session Detection (PSD). Automated log-in/log-out tests are conducted to validate ACS UDIDs are random. **Failure Immediate:** if any UDID session allocations are detected as predictable.

5.5 Platform Conformance

As part of the penetration test procedure all ACS platforms undergo an audit process to validate change characteristics, support readiness, and configuration conformance.

These are as follows (no particular order, role dependent):

1. Versions conformance, including but not limited to Operating System, anti-virus, malware, remote access services, RDP, SCP, SFTP, SMTP, NTP
2. Malware and antivirus scan
3. Accounts, user, email, repository, access, usage
4. Firewall configuration IP, application, and port rules
5. Network configuration, gateway, DNS, DHCP services
6. IP assets, IPtables, routing
7. File assets and sizes,
8. Deleted file assets
9. Driver assets
10. Drive volumes, utilization, and health
11. IP traffic usage, type, and pattern change
12. System event and access logs

6.0 Exhibits

6.1 Excel Incident Report Form (*V3-072022*)

INCIDENT REPORT
Open UTC (yymmddhhmm):
Offending IP Address:
Location of Incident(LOI):
Incident Type(TOI):
Reported by:
Line Manager:
Grade (01-05, lo-hi): IR-
DESCRIPTION OF INCIDENT(DOI)
EMPLOYEE EXPLANATION
WITNESS EXPLANATION
ACTIONS/ESCALATIONS
Lead:

Customer:
Customer Contact:
Customer Impact:
Support Ticket:
IPs Blocked:
Block Confirmed:
ISP Notified:
ISP Customer:
ISP Comments:
Closing Comments: