



BPO Convergence

Monthly IT Evaluation & Testing Report

Sunday, 27 July 2025



All information contained in this document is proprietary of BPO Convergence Pvt Ltd Company. The content, terms, and details of this report, in whole or in part, are strictly confidential and contain intellectual property, information, and ideas owned by BPO Convergence Pvt Ltd. This report or any of its contents may only be used for its internal use and may not be disclosed to any third party without written consent from BPO Convergence Pvt Ltd.

The information in this documentation is subject to change without notice and should not be construed as a commitment by BPO Convergence Pvt Ltd. BPO Convergence Pvt Ltd. makes no representations or warranties, express or implied, with respect to the documentation and shall not be liable for any damages, including any indirect, incidental, consequential damages (such as loss of profit, loss of use of assets, loss of business opportunity, loss of data or claims for or on behalf of user's customers), that may be suffered by the user.

© 2025 – BPO Convergence Pvt. Ltd. India

www.bpoconvergence.com

CONTENTS

| | |
|--|-----------|
| ENGAGEMENT DETAILS: | 3 |
| Limitations on Disclosure and Use of This Report | 5 |
| Confidentiality | 5 |
| SUMMARY: | 6 |
| Vulnerability Summary | 7 |
| Executive Summary | 7 |
| METHODOLOGY: | 9 |
| Assessment Type | 9 |
| Risk Assessment Methodology | 9 |
| FINDINGS TABLE: | 11 |
| Services by Host & by Open Port: | 11 |
| FINDING DETAILS: | 12 |
| Minimal Priority Findings: | 12 |
| 1 – Sensitive Information Disclosure | 12 |

ENGAGEMENT DETAILS:

ASSESSMENT SUMMARY

| | |
|----------------------|--|
| Engagement Timeframe | |
| Assessment ID | SWIGGY, BAJAJ, & AINU_Internal_Network_V4.2- |
| Application Type | Internal Network |
| Authors | Sundaraiah |
| Penetration Tester | Veera, Gulab chandra & Satya |
| Report Version | 4.2 |
| Last Update | 27/07/2025 |

ASSESSMENT SCOPE SUMMARY

The scope of this assessment was limited to components and interfaces specific to Company External Network.

| | |
|------------------------------|--|
| In scope Network Name | Airtel Network |
| In Scope | Antivirus Patch, Domain Status, Policy Update & Others |
| Environment | Production |
| In scope User roles | N/A |
| Out of Scope | Anything Excluding the In Scope IP. |

Limitations on Disclosure and Use of This Report

This report contains information concerning potential vulnerabilities of in-scope network and methods of exploiting them. Organization recommends that special precautions be taken to protect the confidentiality of both this document and the information contained herein.

Security assessment is an uncertain process, based upon past experiences, currently available information, and known threats. It should be understood that all information systems, which by their nature are dependent on human beings, are vulnerable to some degree.

Therefore, while Organization considers the major security vulnerabilities of the analysed network to have been identified, there can be no assurance that any exercise of this nature will identify all possible vulnerabilities or propose exhaustive and operationally viable recommendations to mitigate those exposures.

In addition, the analysis set forth herein is based on the technologies and known threats as of the date of this report. As technologies and risks change over time, the vulnerabilities associated with the operation of the target external network described in this report, as well as the actions necessary to reduce the exposure to such vulnerabilities will also change.

This report may recommend that the target network use certain software or hardware products manufactured or maintained by other vendors.

This report was prepared by Internal IT team for the exclusive use and benefit of target systems and is deemed proprietary information.

Confidentiality

This document contains information that is confidential and proprietary, which shall not be disclosed outside Authorize person/company, transmitted, or duplicated, used in whole or in part for any purpose other than its intended purpose. Any use or disclosure in whole or in part of this information without explicit written permission of network owner is prohibited.

SUMMARY:

This report presents the results of the Security Testing of Scope in network. The purpose of this assessment is to identify network and related network-level security issues that could affect the target network – remediate it before the network is fully launched to its users.

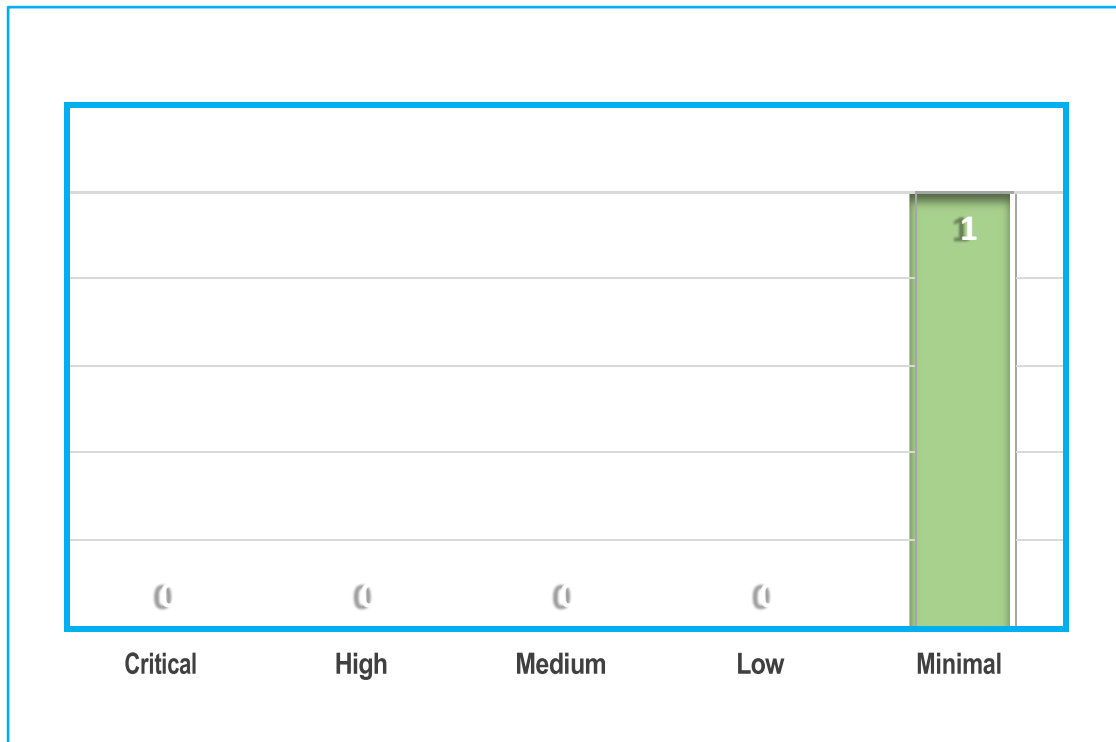
To evaluate the security of the network and network, IT team attempted to perform unauthorized transactions, obtain confidential information, and determine the overall security of the network by performing a wide variety of vulnerability checks.

The testing also included the servers, and technologies associated with the organization and network. This result is intended to be an assessment of the targeted network and any asset that fall within the scope of this project.

Furthermore, the findings in this report reflect the conditions found during the testing, and do not necessarily reflect current conditions. The objective of the analysis is to simulate an attack to assess and discover weak links and provide recommendations and guidelines to vulnerable entities discovered. Every issue includes an overview, issues found and security guidelines, which, if followed correctly, will ensure the confidentiality and integrity of the systems and network.

Vulnerability Summary

The following Number of vulnerabilities were found at each risk level. It is essential to know that total vulnerabilities are not a factor in determining the risk level. The risk level is depending upon the severity of the vulnerabilities found.



Executive Summary

BPO Convergence Pvt Ltd.c conducted Internal Test for “Noida”. This test was performed to assess target systems defensive posture and provide security assistance through proactively identifying vulnerabilities, validating their severity, and providing remediation steps.

Our security assessment revealed ‘1’ vulnerabilities (‘1’ Minimal Risks) in the target Network.

Grading Criteria's:

| Grade | Level | Criteria Description |
|-------|----------------|--|
| A | Excellent | The security exceeds "Industry Best Practice" standards. The overall posture was found to be excellent with only a few low-risk findings identified. |
| B | Good | The security meets with accepted standards for "Industry Best Practice." The overall posture was found to be strong with only a handful of medium- and low- risk shortcomings identified. |
| C | Fair | Current solutions protect some areas of the enterprise from security issues. Moderate changes are required to elevate the discussed areas to "Industry Best Practice" standards. |
| D | Unsatisfactory | Significant security deficiencies exist. Immediate attention should be given to the discussed issues to address exposures identified. Major changes are required to elevate to "Industry Best Practice" standards. |
| E | Inadequate | Serious security deficiencies exist. Shortcomings were identified throughout most or even all of the security controls examined. Improving security will require a major allocation of resources. |

METHODOLOGY:

Assessment Type

IT team was engaged to perform a time-boxed manual security assessment against the target network. This assessment involved a deep automated scan using automated scanning tools to discover common vulnerabilities, as well as manual testing. Manual testing includes validation of all issue types covered under the automated scan as well as checks for problems not typically found by automated scanners.

Risk Assessment Methodology

The severity assigned to each vulnerability was calculated using the NIST 800-30 Revision 1 standard. This standard determines the risk posed by application based on the likelihood an attacker exploits the vulnerability and the impact that it would have on the business.

Likelihood

The difficulty of exploiting the described security vulnerability includes required skill level and the amount of access necessary to visit the element susceptible to the vulnerability. The difficulty is rated with the following values:

Critical: An attacker is almost certain to initiate the threat event.

High: An untrained user could exploit the vulnerability or the vulnerability is very obvious and easily accessible.

Medium: The vulnerability requires some hacking knowledge or access is restricted in some way.

Low: Exploiting the vulnerability requires application access, significant time, resource or a specialized skillset.

Minimal: Adversaries are highly unlikely to leverage the vulnerability.

Impact

The impact the vulnerability would have on the organization if it were successfully exploited is rated with the following values:

Critical: The issue causes multiple severe or catastrophic effects on organizational operations, organizational assets or other organizations.

High: Exploitation produces severe degradation in mission capability to the point that the organization is not able to perform primary functions or results in damage to organizational assets.

Medium: Threat events trigger degradation in mission capability to an extent the application is able to perform its primary functions, but their effectiveness is reduced and there may be damage to organizational assets.

Low: Successful exploitation has limited degradation in mission capability; the organization is able to perform its primary functions, but their effectiveness is noticeably reduced and may result in minor damage to organizational assets.

Minimal: The threat could have a negligible adverse effect on organizational operations or organizational assets.

Severity

The vulnerability severity is determined using the likelihood and impact weights in the following table:

| | | Impact | | | | |
|------------|-----------------|----------------|------------|---------------|-------------|-----------------|
| | | <i>Minimal</i> | <i>Low</i> | <i>Medium</i> | <i>High</i> | <i>Critical</i> |
| Likelihood | <i>Critical</i> | Minimal | Low | Medium | High | Critical |
| | <i>High</i> | Minimal | Low | Medium | High | Critical |
| | <i>Medium</i> | Minimal | Low | Medium | Medium | High |
| | <i>Low</i> | Minimal | Low | Low | Low | Medium |
| | <i>Minimal</i> | Minimal | Minimal | Minimal | Low | Low |

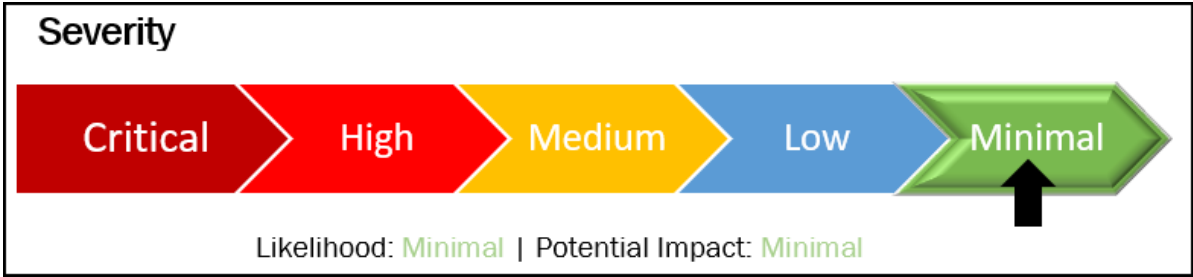
FINDINGS TABLE:

| S.NO | HOST NAME | PORT NUMBER | CHECKLIST | CHECKED BY | DATE |
|------|-----------|-------------|---|------------|------|
| | | | Remote Desktop Connection: | | |
| | | | Remote desktop connection will be disabled on all systems to prevent unauthorized remote access. | | |
| | | | Ctrl + Alt + Del: | | |
| | | | The Ctrl + Alt + Del function will be enabled on the lock screen, ensuring that users must authenticate before any further actions are taken on the system. | | |
| | | | Microsoft Store: | | |
| | | | The Microsoft Store will be disabled to prevent the installation of unauthorized applications or software. | | |
| | | | Command Prompt (CMD): | | |
| | | | The CMD (Command Prompt) will be disabled to prevent users from executing potentially harmful or unauthorized commands on the system with process requirement. | | |
| | | | Snipping Tool: | | |
| | | | The Snipping Tool will be disabled to restrict the ability to capture sensitive screen data or images based upon requirement. | | |
| | | | Antivirus: | | |
| | | | The antivirus software will be disabled only if explicitly approved or if managed through centralized security systems. No user-level disabling of antivirus will be allowed. | | |
| | | | Approved Applications: | | |
| | | | Only the following applications will be allowed on systems: | | |
| | | | Microsoft Office Suite (for supervisors only) | | |
| | | | Excel 2010 or 2016 (for approved users) | | |
| | | | No other applications should be installed or accessible without prior approval from IT | | |

FINDING DETAILS:

Minimal Priority Findings:

1 – Sensitive Information Disclosure



Description:

This vulnerability occurs when sensitive information is inadvertently disclosed through an open network port, allowing unauthorized parties to access and potentially exploit this information.

Consequence:

Attackers can use this information to compromise the security of the system and potentially steal confidential data or disrupt services.

Instances:

1) Location – Hyderabad

Process- SWIGGY-HYD

| SR.NO | END POINT NAME | GROUP | POLICY | DOMIN | STATUS | DATABASE UPDATE DATE |
|-------|----------------|-----------|--------|----------------|--------|----------------------|
| 1 | HYD-SWG-0010 | Hyderabad | HYD | BPOCSWIGGY.COM | ACTIVE | 27-July-25 |
| 2 | HYD-SWG-0011 | Hyderabad | HYD | BPOCSWIGGY.COM | ACTIVE | 27-July-25 |
| 3 | HYD-SWG-0012 | Hyderabad | HYD | BPOCSWIGGY.COM | ACTIVE | 27-July-25 |
| 4 | HYD-SWG-0013 | Hyderabad | HYD | BPOCSWIGGY.COM | ACTIVE | 27-July-25 |
| 5 | HYD-SWG-0014 | Hyderabad | HYD | BPOCSWIGGY.COM | ACTIVE | 27-July-25 |
| 6 | HYD-SWG-001 | Hyderabad | HYD | BPOCSWIGGY.COM | ACTIVE | 27-July-25 |
| 7 | HYD-SWG-002 | Hyderabad | HYD | BPOCSWIGGY.COM | ACTIVE | 27-July-25 |
| 8 | HYD-SWG-003 | Hyderabad | HYD | BPOCSWIGGY.COM | ACTIVE | 27-July-25 |
| 9 | HYD-SWG-004 | Hyderabad | HYD | BPOCSWIGGY.COM | ACTIVE | 27-July-25 |
| 10 | HYD-SWG-0045 | Hyderabad | HYD | BPOCSWIGGY.COM | ACTIVE | 27-July-25 |
| 11 | HYD-SWG-005 | Hyderabad | HYD | BPOCSWIGGY.COM | ACTIVE | 27-July-25 |
| 12 | HYD-SWG-006 | Hyderabad | HYD | BPOCSWIGGY.COM | ACTIVE | 27-July-25 |
| 13 | HYD-SWG-007 | Hyderabad | HYD | BPOCSWIGGY.COM | ACTIVE | 27-July-25 |

| | | | | | | |
|----|--------------|-----------|-----|----------------|--------|------------|
| 14 | HYD-SWG-008 | Hyderabad | HYD | BPOCSWIGGY.COM | ACTIVE | 27-July-25 |
| 15 | HYD-SWG-009 | Hyderabad | HYD | BPOCSWIGGY.COM | ACTIVE | 27-July-25 |
| 16 | HYD-SWG-015 | Hyderabad | HYD | BPOCSWIGGY.COM | ACTIVE | 27-July-25 |
| 17 | HYD-SWG-016 | Hyderabad | HYD | BPOCSWIGGY.COM | ACTIVE | 27-July-25 |
| 18 | HYD-SWG-017 | Hyderabad | HYD | BPOCSWIGGY.COM | ACTIVE | 27-July-25 |
| 19 | HYD-SWG-018 | Hyderabad | HYD | BPOCSWIGGY.COM | ACTIVE | 27-July-25 |
| 20 | HYD-SWG-019 | Hyderabad | HYD | BPOCSWIGGY.COM | ACTIVE | 27-July-25 |
| 21 | HYD-SWG-021 | Hyderabad | HYD | BPOCSWIGGY.COM | ACTIVE | 27-July-25 |
| 22 | HYD-SWG-026 | Hyderabad | HYD | BPOCSWIGGY.COM | ACTIVE | 27-July-25 |
| 23 | HYD-SWG-027 | Hyderabad | HYD | BPOCSWIGGY.COM | ACTIVE | 27-July-25 |
| 24 | HYD-SWG-028 | Hyderabad | HYD | BPOCSWIGGY.COM | ACTIVE | 27-July-25 |
| 25 | HYD-SWG-029 | Hyderabad | HYD | BPOCSWIGGY.COM | ACTIVE | 27-July-25 |
| 26 | HYD-SWG-030 | Hyderabad | HYD | BPOCSWIGGY.COM | ACTIVE | 27-July-25 |
| 27 | HYD-SWG-031 | Hyderabad | HYD | BPOCSWIGGY.COM | ACTIVE | 27-July-25 |
| 28 | HYD-SWG-032 | Hyderabad | HYD | BPOCSWIGGY.COM | ACTIVE | 27-July-25 |
| 29 | HYD-SWG-033 | Hyderabad | HYD | BPOCSWIGGY.COM | ACTIVE | 27-July-25 |
| 30 | HYD-SWG-034 | Hyderabad | HYD | BPOCSWIGGY.COM | ACTIVE | 27-July-25 |
| 31 | HYD-SWG-035 | Hyderabad | HYD | BPOCSWIGGY.COM | ACTIVE | 27-July-25 |
| 32 | HYD-SWG-036 | Hyderabad | HYD | BPOCSWIGGY.COM | ACTIVE | 27-July-25 |
| 33 | HYD-SWG-036a | Hyderabad | HYD | BPOCSWIGGY.COM | ACTIVE | 27-July-25 |
| 34 | HYD-SWG-037a | Hyderabad | HYD | BPOCSWIGGY.COM | ACTIVE | 27-July-25 |
| 35 | HYD-SWG-039 | Hyderabad | HYD | BPOCSWIGGY.COM | ACTIVE | 27-July-25 |
| 36 | HYD-SWG-040 | Hyderabad | HYD | BPOCSWIGGY.COM | ACTIVE | 27-July-25 |
| 37 | HYD-SWG-040a | Hyderabad | HYD | BPOCSWIGGY.COM | ACTIVE | 27-July-25 |
| 38 | HYD-SWG-041 | Hyderabad | HYD | BPOCSWIGGY.COM | ACTIVE | 27-July-25 |
| 39 | HYD-SWG-041a | Hyderabad | HYD | BPOCSWIGGY.COM | ACTIVE | 27-July-25 |
| 40 | HYD-SWG-042 | Hyderabad | HYD | BPOCSWIGGY.COM | ACTIVE | 27-July-25 |
| 41 | HYD-SWG-042a | Hyderabad | HYD | BPOCSWIGGY.COM | ACTIVE | 27-July-25 |
| 42 | HYD-SWG-043 | Hyderabad | HYD | BPOCSWIGGY.COM | ACTIVE | 27-July-25 |
| 43 | HYD-SWG-043a | Hyderabad | HYD | BPOCSWIGGY.COM | ACTIVE | 27-July-25 |
| 44 | HYD-SWG-044 | Hyderabad | HYD | BPOCSWIGGY.COM | ACTIVE | 27-July-25 |

Process- **BAJAJ-HYD**

| SR.NO | END POINT NAME | GROUP | POLICY | STATUS | DATABSE UPDATE DATE |
|-------|----------------|-----------|-----------|--------|---------------------|
| 1 | HYD-BAJ-03 | Bajaj Guw | Bajaj_Guw | ACTIVE | 27-July-25 |
| 2 | HYD-BAJ-04 | Bajaj Guw | Bajaj_Guw | ACTIVE | 27-July-25 |
| 3 | HYD-BAJ-05 | Bajaj Guw | Bajaj_Guw | ACTIVE | 27-July-25 |
| 4 | HYD-BAJ-06 | Bajaj Guw | Bajaj_Guw | ACTIVE | 27-July-25 |
| 5 | HYD-BAJ-07 | Bajaj Guw | Bajaj_Guw | ACTIVE | 27-July-25 |
| 6 | HYD-BAJ-08 | Bajaj Guw | Bajaj_Guw | ACTIVE | 27-July-25 |
| 7 | HYD-BAJ-09 | Bajaj Guw | Bajaj_Guw | ACTIVE | 27-July-25 |
| 8 | HYD-BAJ-10 | Bajaj Guw | Bajaj_Guw | ACTIVE | 27-July-25 |
| 9 | HYD-BAJ-11 | Bajaj Guw | Bajaj_Guw | ACTIVE | 27-July-25 |
| 10 | HYD-BAJ-12 | Bajaj Guw | Bajaj_Guw | ACTIVE | 27-July-25 |
| 11 | HYD-BAJ-13 | Bajaj Guw | Bajaj_Guw | ACTIVE | 27-July-25 |
| 12 | HYD-BAJ-14 | Bajaj Guw | Bajaj_Guw | ACTIVE | 27-July-25 |
| 13 | HYD-BAJ-15 | Bajaj Guw | Bajaj_Guw | ACTIVE | 27-July-25 |
| 14 | HYD-BAJ-16 | Bajaj Guw | Bajaj_Guw | ACTIVE | 27-July-25 |
| 15 | HYD-BAJ-17 | Bajaj Guw | Bajaj_Guw | ACTIVE | 27-July-25 |
| 16 | HYD-BAJ-18 | Bajaj Guw | Bajaj_Guw | ACTIVE | 27-July-25 |
| 17 | HYD-BAJ-19 | Bajaj Guw | Bajaj_Guw | ACTIVE | 27-July-25 |
| 18 | HYD-BAJ-21 | Bajaj Guw | Bajaj_Guw | ACTIVE | 27-July-25 |
| 19 | HYD-BAJ-22 | Bajaj Guw | Bajaj_Guw | ACTIVE | 27-July-25 |
| 20 | HYD-BAJ-24 | Bajaj Guw | Bajaj_Guw | ACTIVE | 27-July-25 |
| 21 | HYD-BAJ-25 | Bajaj Guw | Bajaj_Guw | ACTIVE | 27-July-25 |
| 22 | HYD-BAJ-26 | Bajaj Guw | Bajaj_Guw | ACTIVE | 27-July-25 |
| 23 | HYD-BAJ-27 | Bajaj Guw | Bajaj_Guw | ACTIVE | 27-July-25 |
| 24 | HYD-BAJ-012 | Bajaj Guw | Bajaj_Guw | ACTIVE | 27-July-25 |
| 25 | HYD-BAJ-040 | Bajaj Guw | Bajaj_Guw | ACTIVE | 27-July-25 |

Process- **AINU-HYD**

| SR.NO | END POINT NAME | GROUP | POLICY | STATUS | DATABSE UPDATE DATE |
|-------|----------------|----------|----------|--------|---------------------|
| 1 | HYD-AINU-001 | AINU_HYD | AINU_HYD | ACTIVE | 27-July-25 |
| 2 | HYD-AINU-002 | AINU_HYD | AINU_HYD | ACTIVE | 27-July-25 |
| 3 | HYD-AINU-003 | AINU_HYD | AINU_HYD | ACTIVE | 27-July-25 |
| 4 | HYD-AINU-004 | AINU_HYD | AINU_HYD | ACTIVE | 27-July-25 |
| 5 | HYD-AINU-005 | AINU_HYD | AINU_HYD | ACTIVE | 27-July-25 |
| 6 | HYD-AINU-006 | AINU_HYD | AINU_HYD | ACTIVE | 27-July-25 |
| 7 | HYD-AINU-007 | AINU_HYD | AINU_HYD | ACTIVE | 27-July-25 |
| 8 | HYD-AINU-008 | AINU_HYD | AINU_HYD | ACTIVE | 27-July-25 |
| 9 | HYD-AINU-009 | AINU_HYD | AINU_HYD | ACTIVE | 27-July-25 |
| 10 | HYD-AINU-010 | AINU_HYD | AINU_HYD | ACTIVE | 27-July-25 |
| 11 | HYD-AINU-011 | AINU_HYD | AINU_HYD | ACTIVE | 27-July-25 |
| 12 | HYD-AINU-012 | AINU_HYD | AINU_HYD | ACTIVE | 27-July-25 |

| | | | | | |
|----|--------------|----------|----------|--------|------------|
| 13 | HYD-AINU-013 | AINU_HYD | AINU_HYD | ACTIVE | 27-July-25 |
| 14 | HYD-AINU-014 | AINU_HYD | AINU_HYD | ACTIVE | 27-July-25 |
| 15 | HYD-AINU-015 | AINU_HYD | AINU_HYD | ACTIVE | 27-July-25 |
| 16 | HYD-AINU-016 | AINU_HYD | AINU_HYD | ACTIVE | 27-July-25 |

WAY AHEAD:

A detailed plan for closure of the gaps found during this review should be created. Network must be re-tested, before moving the new code into production environment. A periodic monitoring mechanism should be instituted to ensure compliance levels are maintained all the time. BPO Convergence Pvt Ltd. is happy to perform periodic assessments once in a quarter or whenever there is a major code change or when industry consortiums report new vulnerabilities or threats, whichever comes first.

APPENDIX 1: EXTERNAL NETWORK SECURITY ASSESSMENT TASK

An indicative list of tasks conducted for a web application assessment, in addition to the application's requirements;

- ✓ **Vulnerability Scanning** – Using automated tools to scan the target network for known vulnerabilities, which can include outdated software, unpatched systems, and misconfigured devices.
- ✓ **Network Mapping** - Mapping the network to identify all devices and systems on the network, including their IP addresses, operating systems, and services running.
- ✓ **Port Scanning** - Using automated tools to scan all open ports on the target network to identify any unauthorized services, applications or open ports that may be vulnerable to attack.
- ✓ **Exploitation Testing**: Testing for exploitable vulnerabilities identified during the vulnerability scanning and port scanning phases using manual and automated tools to verify their existence.
- ✓ **Password Cracking**: Testing the strength of passwords used within the network and identifying any weak or easily guessable passwords which can be used to gain unauthorized access.
- ✓ **Firewall Testing**: Testing the security of the firewall configuration to identify any misconfigured rules or policies that may be exploited.
- ✓ **Denial of Service (DoS) Testing**: Testing the resilience of the network against Denial-of-Service attacks that can cause network outages.

ABOUT US

BPO Convergence Pvt. Ltd., a Fornax Company, is a Business Process Management (BPM) company specializing in customer experience management, managed services, analytics, staffing solutions, and transaction processing, with a focus on delivering cost-effective and sustainable solutions

For more information, visit us at www.bpoconvergence.com