Government of India
Ministry of Electronics & Information Technology
Standardisation, Testing & Quality Certification Directorate
Electronics Niketan, 6 CGO Complex, Lodhi Road, New Delhi-110020.

भारतसरकार
इलेक्ट्रॉनिकीऔरसूचनाप्रौद्योगिकीमंत्रालय
मानकीकरण, परीक्षणएवंगुणवत्ताप्रमाणननिदेशालय
इलेक्ट्रॉनिक्सनिकेतन, 6, सीजीओकॉम्प्लेक्स, लोधीरोड, नईदिल्ली - 110003

WEB APPLICATION SECURITY COMPLIANCE STATUS

Ref. Test Report No.: ITBg/WAS(TR)-1/IT16990525/4   **Dated: 08/05/2025**

Name of Test Laboratory: STQC IT Services, Agartala

Identification of Web Application: APT 2.0 version 1.0

Tested Modules: PAO Accounts, IDAM MDM & Integrations, Customers Portals

Organization Name: Department of Post, DAK Bhawan, Parliament Street, New Delhi-110001

Test / Staging URL: https://sit.indiapost.gov.in/enterpriseportal

Production URL:https://app.indiapost.gov.in/employeeportal

Date of Testing: Start Date: 29/04/2025to End Date: 05/05/2025

TEST RESULT SUMMARY:

OWASP Top10	Web Application Vulnerabilities	Compliance	Remark
A01:2021	Broken Access Control	Satisfactory	--
A02:2021	Cryptographic Failures	Satisfactory	--
A03:2021	Injection	Satisfactory	--
A04:2021	Insecure Design	Satisfactory	--
A05:2021	Security Misconfiguration	Satisfactory	--
A06:2021	Vulnerable and Outdated Components	Satisfactory	--
A07:2021	Identification and Authentication Failures	Satisfactory	--
A08:2021	Software and Data Integrity Failures	Satisfactory	--
A09:2021	Security Logging and Monitoring Failures	Satisfactory	--
A10:2021	Server-Side Request Forgery	Satisfactory	--

RECOMMENDATIONS:

1. The web application is recommended to be hosted at **https://app.indiapost.gov.in/employeeportal** with 'Read Only permission'.
2. Security hardening / secured configuration of the Web Server, Network devices and Operating System are recommended for the hosting environment.
3. Regular security vulnerability assessment of the hosting IT infrastructure (servers and network devices) is recommended.

CONCLUSION:

- This statement of compliance is issued for the specific version of the Web Application.
- This Statement of compliance becomes null and void, if changes are made to the Application code related to the security architecture & security mechanisms for handling inputs, user Access Control, user Authentication & Authorization, Session Management, handling sensitive data, Data encryption at Rest & in Motion, handling of runtime errors & external resources.
- This statement of compliance state is also become null and void if there is any change in underlying IT infrastructure or their configuration, hosting the Web Application and if any new vulnerabilities are discovered.

Issued By:

T. Birunjit Singh
Scientist "B", STQC, IT Agartala