Synapxe Vulnerability Disclosure Programme Policy

Purpose

This policy gives security researchers and other participants clear guidelines under the Synapxe Vulnerability Disclosure Programme (VDP) in the responsible reporting of suspected vulnerabilities or weaknesses in Synapxe's and/or public healthcare entities' IT services, systems, websites which may potentially affect public healthcare's internet-accessible websites/applications.

As part of our continuing approach in proactively discovering and remediating security vulnerabilities on our Public Healthcare Digital assets, Synapxe on behalf of the Public Healthcare entities* in Singapore has embarked on this Vulnerability Disclosure Programme (VDP) with Hackerone; to identify these vulnerabilities and address them before they are exploited by malicious threat actors.

Participation in the programme is voluntary and is subject to the terms and conditions listed on this page. By submitting a report, you acknowledge and agree to the terms and conditions listed in this Policy. You will also acknowledge that, as long as they are not inconsistent with this Policy; you are subject to:

- HackerOne's Disclosure Guidelines
- Finder Terms and Conditions
- General Terms and Conditions

Response Targets

We will make a best effort to meet the following SLAs for hackers participating in our programme:

Type of Response	SLA in business days
First Response	1 days
Time to Triage	7 days
Time to Resolution	depends on severity and complexity

We'll try to keep you informed about our progress throughout the process.

Programme Rules

1. Please provide detailed reports with reproducible steps. If the report is not detailed enough to reproduce the issue, it will be rejected.
2. We reserve the right to amend this Policy Statement at any time at our sole and absolute discretion without any advance notice. Your participation and continued participation in the VDP constitutes your acknowledgement and acceptance of the amendments.
3. You shall not take any action which may contravene applicable laws and regulations (e.g. Computer Misuse Act). For the avoidance of doubt, attempts to exploit or test vulnerabilities (e.g. gaining unauthorised access to any computer programme or data) are prohibited.
4. Expected Conduct. You are expected to conduct yourself responsibly at all times and, as a non-exhaustive guide, you shall:

   a. Act responsibly, with the main purpose of reporting vulnerabilities and safeguarding our assets from harm.
   b. Refrain from causing any kind of harm to individuals or organisations (e.g. do not attempt to test, reproduce or verify a vulnerability, or take action which may cause interruption or degradation of digital services).
   c. Conduct yourself in accordance with all applicable laws and regulations at all times. Do obtain professional legal advice if you have any doubt about such laws or regulations.
   d. Upon detection of a vulnerability, notify us immediately or as soon as practicable by submitting a report through the HackerOne platform on this vulnerability. Under no circumstances should you attempt to exfiltrate any computer data or publish details of any vulnerability.
   e. Provide adequate information in the vulnerability report to help us validate the vulnerability, including these details (where applicable):
      i. Description of the vulnerability.
      ii. IP address and/or URL.
      iii. Configuration and version of the software.
      iv. Description of the circumstances, including date(s) and time(s), leading to your reporting of the vulnerability. v. Description of the reason(s) why you believe the vulnerability may impact the services and the extent of such potential impact (e.g. describe how you believe the vulnerability might potentially operate).
   f. Do not try to further pivot into the network by using a vulnerability. The standard rules around Remote Code Execution (RCE), SQL Injection (SQLi), and FileUpload vulnerabilities as specified by Hackerone shall apply and can be found in RCESQLandFileUploadRestrictions(1).pdf (F2548636).

g. Do not try to exploit service providers we use; prohibited actions include, but are not limited to, bruteforcing login credentials of Domain Registrars, DNS Hosting Companies, Email Providers and/or others. You are prohibited from performing any actions to or against any property/system/service/data not in scope for this programme as specified in this policy.
h. If you encounter Personally Identifiable Information (PII), you must contact us immediately. Do not proceed with access and immediately purge any local information, if applicable.
i. Please limit any automated scanning to 60 requests per second. Aggressive testing that causes service degradation will be grounds for removal from the programme.
j. Submit one vulnerability per report, unless you need to chain vulnerabilities to provide impact.
k. After validating your submitted vulnerability report, we may at our sole discretion provide appropriate recognition to you for your contribution. However, we will not provide any cash reward/bounty of any kind for the validated vulnerability.
l. When duplicates occur, the recognition will only be accorded to the first report that was received and validated.
m. Only one recognition will be accorded for multiple vulnerabilities caused by one underlying issue.
n. Use best efforts to avoid any privacy violation, data breach, destruction of data, and/or interruption or degradation of our service.

Prohibited Conduct

You are expected to conduct yourself responsibly at all times, which shall include (but is not limited to) not performing any of the following acts:

1. Act in any way which may contravene applicable laws and regulations (e.g. the Computer Misuse Act).
2. Discuss any vulnerabilities (even resolved ones) outside of the programme without express consent from the organisation. Publish or publicly disclose any vulnerability to any third party; you may however disclose any vulnerability to us through the approved communication channel.
3. Deploy destructive, disruptive and/or unlawful means to detect vulnerabilities (e.g. attacks on physical security, denial of service, brute force attacks and/or use of malicious software). Social engineering (e.g. phishing, vishing, smishing and/or other forms of deception against our employees, contractors or third parties) is strictly prohibited.
4. Exploit, test or otherwise use any vulnerability (e.g. taking any step(s) to access, copy, create, delete, modify, manipulate or download any data or programme,

to build system backdoor(s), to modify system configuration(s), and/or to facilitate or share system access).

Out of scope vulnerabilities

The following issues are considered out of scope:

1. Disruption of our service (DoS, DDoS)
2. PII - do not collect any personally identifiable information - including credit card information, addresses and phone numbers.
3. Reports from automated tools or scans
4. 0-day vulnerabilities younger than 60 days
5. Social engineering of employees or contractors or third parties
6. Missing security best practices and controls (rate-limiting/throttling, lack of CSRF protection, lack of security headers, missing flags on cookies, descriptive errors, server/technology disclosure - without clear and working exploit)
7. Self-exploitation (cookie reuse, self cookie-bomb, self denial-of-service etc.)
8. Self Cross-site Scripting vulnerabilities without evidence on how the vulnerability can be used to attack another user
9. Lack of HTTPS
10. Server Banner Disclosure/Technology used Disclosure
11. Clickjacking
12. CSS Injection attacks (Unless it gives you ability to read anti-CSRF tokens or other sensitive information)
13. Tabnabbing
14. Reflective File Download
15. Open ports which do not lead directly to a vulnerability
16. Any physical/wireless attempt against our property or data centers
17. Violations of secure design principles which are not part of exploitable vulnerabilities
18. CSRF on forms available to anonymous users (e.g. contact forms and logout).
19. HTTP/TLS configuration issues without demonstrable impact (e.g. TLS configuration issues such as BEAST, BREACH, renegotiation attacks, insecure cipher suites; missing HTTP security headers; lack of Secure or HTTPOnly cookie flags)
20. Presence or absence of application/browser autocomplete or save-password flags
21. Username enumeration on login or forgot password pages
22. Reports about missing rate limiting where other mitigations exist (e.g. brute force attacks against login pages already protected by multi-factor authentication)
23. Clickjacking attacks which do not lead to any sensitive state stages

24. HTTP OPTIONS/TRACE methods enabled
25. Thirdparty owned vulnerabilities – e.g. Sharepoint
26. Known Vulnerabilities

Safe Harbour

This policy is designed to be compatible with common vulnerability disclosure good practice. It does not give you permission to act in any manner that is inconsistent with the law, or which might cause us (or you) to be in breach of any of our (or your) legal obligations, including but not limited to:

- Computer Misuse Act and Personal Data Protection Act
- Any other law applicable to us and/or you (including, where applicable, General Data Protection Regulation 2016/679 (EU GDPR) and the UK Data Protection Act 2018)

We affirm that we will not seek prosecution of any security researcher who reports any security vulnerability on a service or system, where the researcher has acted in good faith and in accordance with this policy. However, do note that we will not:

i. Accord or provide you with any kind of exemption, immunity, indemnity or protection from civil or criminal liability (if any) under applicable laws and regulations.
ii. Be liable for any liability, expense, damage, cost or loss of any kind which you may incur due to any action taken or not taken by us in relation to any vulnerability you may report.
iii. Accept or assume any responsibility for the contents of any vulnerability report submitted by you, nor shall our acknowledgment or processing of such report constitute any kind of acceptance or endorsement of the contents therein.
iv. Be obliged to consult you for any media or public statement that we and/or any stakeholders may decide to publish or release in relation to the vulnerability, or provide you with any form of public recognition. We cannot authorise any activity on or against third-party products and cannot guarantee that third parties (including vendors) will not pursue legal action against you. We shall not be held responsible or liable for any liability, claim, loss, cost and/or expense that you may incur arising out of or in connection with any actions performed on or against any third party.

Governing Law and Dispute Resolution

This policy shall be subject to, governed by and construed in all respects in accordance with Singapore law. You and us hereby submit to the exclusive jurisdiction of the

Singapore Courts to resolve any dispute arising out of or in connection with or in relation to this policy.

Thank you for helping keep us and our users safe!

*Public Healthcare entities in Scope

Entity	Corporate Website for Background information
Singapore Health Services (SingHealth)	www.singhealth.com.sg
National University Health System (NUHS)	www.nuhs.edu.sg
National Healthcare Group (NHG)	https://corp.nhg.com.sg
1 Finance Shared Services (1FSS)	www.1fss.com.sg
Agency for Integrated Care (AIC) / Intermediate & long term care (ILTC) services	www.aic.sg
ALPS Healthcare (ALPS)	www.alpshealthcare.com.sg
Synapxe	www.synapxe.sg
MOH Holdings (MOHH)	www.mohh.com.sg