# WORK ORDER

1) Once signed by the Suncorp Group company named in this Order and the Supplier, this Order creates a binding agreement between that Suncorp Group company and the Supplier consisting of the terms of this Order, any documents referred to in this Order and the terms of the Agreement.
2) In the agreement formed between a Suncorp Group company and the Supplier, references in the constituent documents of that agreement to 'Suncorp' shall be deemed to be references to that Suncorp Group company.
3) All clause numbers in the headings and titles in this Order are references to clause numbers in the Agreement.

**IMPORTANT: This Work Order template may only be used when there is a valid (executed and current) overarching Master Agreement established with the supplier.**

| **1. Order Details** | |
|---|---|
| **1.1 Order Title/Description** | Penetration Testing Services |
| **1.2 Order Number** | |
| **1.3 Agreement Number** | CW57433 |
| **1.4 Name of Supplier** | DELOITTE TOUCHE TOHMATSU ABN 74 490 121 060 |
| **1.5 Name of Suncorp Group company executing Order** | Suncorp Corporate Services Pty Ltd ABN 69 074 966 466 |
| **1.6 Suncorp Project Officer** | Mia BRDANOVIC<br>Security Analyst<br>Security Assurance<br>T 0413 920 582 |
| **1.7 Supplier Contract Manager** | Jarrod Oakley<br>Partner \| Deloitte Risk Advisory<br>M: +61 411 703 688 |
| **1.8 Suncorp office location** | Level 26, Riverside Centre, 123 Eagle Street, Brisbane. Queensland, 4000 |
| **1.9 Service Commencement Date** | 12/10/2022 |
| **1.10 Service Period** | 2 Days |
| **1.11 Working hours** | 9.00 am to 5.30 pm with 1-hour lunch |

## 2. Services

**Suncorp One Suncorp Portal API Penetration Testing**

One Suncorp Portal (OSP) is a space where customers will be able to link/launch to existing pages/portals. OSP is web portal only and equivalent mobile app is the marketplace mobile app but they are different independent applications. The testing will focus on the following new APIs:

- POST – OSP GI Motor Policy One Off Payment
- POST – OSP GI Home Policy One Off Payment

**API Testing Methodology**

While Application Programming Interfaces (APIs) share a lot of functional similarities with a standard web application, they are designed to operate behind the scenes – for either server-to-server or client-to-server communication. As there is no distinct user interface for an API, penetration testing focuses more on how the data and requests are handled and manipulated.

Our penetration testing assessment methodology incorporates the suggested testing techniques from standard methodologies, such as the Web Application Hackers Handbook (WAHH) and OWASP (Open Web Application Security Project) Testing Guide.
These methodologies will cover common vulnerabilities, as highlighted in the OWASP API Security Top 10 2019 (https://owasp.org/www-project-api-security/). Any customization of further testing will be evaluated during the testing period and is different for each API.

**Activities**

Some of the specific test cases that will be covered for this testing are listed below:

- Broken Authentication & Authorization (on Object & Function level)
- Injection
- Improper Assets Management
- Excessive Data Exposure
- Lack of Resources & Rate Limiting
- Security Misconfiguration
- Insufficient Logging & Monitoring

## 3. Deliverables

**Report**

We will provide you with a report detailing the results of the testing performed. This report will include the following key sections:

- **Executive summary:** An overview of the security level of the systems tested, including major vulnerabilities and areas where the general approach to security needs to be improved. We explain the implications of our findings within the context of Suncorp and provide an overall rating of security within the environment tested.
- **Summary of Findings:** A more detailed breakdown of the vulnerabilities and weaknesses identified for each portion of the engagement. We provide an explanation of the finding, as well as the associated risk to Suncorp.
- **Detailed findings:** A detailed description of exposures and their context, together with supporting documentation. We assess the impact and associated risk of each identified exposure and make prioritised technical recommendations to be implemented to address the identified exposures. The priorities and 'Detailed findings' section will also be supported by technical appendices where required.

Final report will be delivered in 5 days from the testing completion date. Any critical or High findings will be reported immediately.

## 4. Equipment to be provided by Supplier

TBD with Suncorp.

## 5. Reporting requirements

| Report Name | Details of required content | Due date/interval |
|---|---|---|
| Suncorp One Suncorp Portal API Penetration Testing Report | Refer section 3 | Final report will be delivered in 5 days from the testing completion date. Any critical or High findings will be reported immediately. |

## 6. Equipment to be provided by Suncorp

Access to environments

## 7. Supplier's Nominated Personnel

| Position description | Names |
|---|---|
| TBA | **Core Team**<br>**Ashish Mahajan**<br>National Director \| Cyber Detect and Response<br>Deloitte Risk Advisory Pty Ltd<br>M: +61 428280129<br><br>**Andy Yang**<br>Specialist Director \| Cyber Detect and Response<br>Deloitte Risk Advisory Pty Ltd<br>M: +61 466 508 806<br><br>**Jared Piconi**<br>Senior Specialist \| Cyber Detect and Response<br>Deloitte Risk Advisory Pty Ltd<br>M: +61 438 740 800<br><br>We will discuss with the Suncorp pentest team and assign resources based on the engagement and availability. |

## 8. Fees and invoicing

| Resource | Daily Rate (excluding GST) |
|---|---|
| Senior Pentester | $1,580 |
| Pentester | $1,580 |

Estimated fees based on **2 days**: **$3,160 excluding GST**

## 9. Expense authority arrangements

The Agreement provides that Personnel providing Services must obtain prior written authority for all expenses. If this is what's required, state here "In accordance with the Agreement". Otherwise, enter details of expense authority limits, and any other rules, rates, or requirements relevant to expenses.

## 10. None

No

| 11. Intellectual Property |
|---|
| (Suncorp and Supplier must consider the Deliverables to be produced under this Order and decide whether the provisions in the Agreement regarding the ownership or licence of those Deliverables are to apply or need to be varied) |

[Note: This Order must be executed in accordance with the Document Execution Standard. An execution block for Power of Attorneys is included below. Please delete which execution block is not applicable]

| 12. Signing | |
|---|---|
| **SUNCORP** | **SUPPLIER** |
| **SIGNED** for and on behalf of **SUNCORP** by:<br><br>Name (print): _____<br><br>Signature: _____<br>Authorised Person<br><br>Date signed: _____<br><br>**AND**:<br><br>Name (print): _____<br><br>Signature: _____<br>Authorised Person<br><br>Date signed: _____ | **SIGNED** for and on behalf of **SUPPLIER** by:<br><br>Name (print): _____<br><br>Signature: _____<br>Partner<br><br>Date signed: _____<br><br>**AND:**<br><br>Name (print): Ashish Mahajan _____<br><br>X _____<br>Ashish Mahajan<br><br>Signature:<br>Director<br><br>Date signed: _____ |