TSP Vulnerability Disclosure Policy

Brand Promise

TSP, an award-winning and customer-endorsed technology solutions company, is committed to ensuring the safety and security of our customers. Toward this end, TSP is now formalizing our policy for accepting vulnerability reports related to our products. We hope to foster an open partnership with the security community, and we recognize that the work the community does is important in continuing to ensure safety and security for all our customers.

We have developed this policy to both reflect our corporate values and to uphold our legal responsibility to good-faith security researchers that are providing us with their expertise.

Initial Program and Scope

Initial Scope
TSP's Vulnerability Disclosure Program initially covers the following products:

- CSC
- TSP Mobile App
- TSP Corporate Network
- TSP Microsoft 365

While TSP offers several other products, we ask that all security researchers submit vulnerability reports only for the stated product list. We intend to increase our scope as we build capacity and experience with this process.

Researchers who submit a vulnerability report to us will be given full credit on our website once the submission has been accepted and validated by our product security team.

We Will Not Take Legal Action If...

Legal Posture
TSP will not engage in legal action against individuals who submit vulnerability reports through our vulnerability reporting program. We openly accept reports for the currently listed TSP products.

We agree not to pursue legal action against individuals who:

- Engage in testing of systems/research without harming TSP or our customers.
- Engage in vulnerability testing within the scope of our vulnerability disclosure program.
- Test on products without affecting customers, or receive permission/consent from customers before engaging in vulnerability testing against their devices/software, etc.
- Adhere to the laws of their location and the location of TSP. For example, violating laws that would only result in a claim by TSP (and not a criminal claim) may be acceptable as TSP is authorizing the activity (reverse engineering or circumventing protective measures) to improve its system.
- Refrain from disclosing vulnerability details to the public before a mutually agreed-upon timeframe expires.

Communication Mechanisms and Process

How to Submit a Vulnerability
To submit a vulnerability report to TSP's Product Security Team, please send email to vdp@mytsp.net.

Nonbinding Submission Preferences and Prioritization

Preference, Prioritization, and Acceptance Criteria
We will use the following criteria to prioritize and triage submissions.

What we would like to see from you:

- Well-written reports in English will have a higher chance of resolution.
- Reports that include proof--of--concept code equip us to better triage.
- Reports that include only crash dumps or other automated tool output may receive lower priority.
- Reports that include products not on the initial scope list may receive lower priority.
- Please include how you found the bug, the impact, and any potential remediation.
- Please include any plans or intentions for public disclosure.

What you can expect from us:

- A timely response to your email (within 2 business days).
- After triage, we will send an expected timeline, and commit to being as transparent as possible about the remediation timeline as well as on issues or challenges that may extend it.
- An open dialog to discuss issues.
- Notification when the vulnerability analysis has completed each stage of our review.
- Credit after the vulnerability has been validated and fixed.

If we are unable to resolve communication issues or other problems, TSP may bring in a neutral third party to assist in determining how best to handle the vulnerability.

Versioning

This document Version 1.0 was created November 3, 2020. Any updates will be noted below in the version notes.