Transport for London

Security and risk management guideline

Purpose

Delivering secure services is our highest priority. We want our customers to enjoy a secure online experience and to that end you must design and code for security and also pass security penetration testing to prevent vulnerabilities which could be exploited to attack TfL's hosting infrastructure, online applications or online services. This document is intended to make you aware of that all of TfL's sites and services must be developed to be secure.

Audience

- Developers
- Testing teams
- Project managers
- Customers
- Anyone engaged in design, development, implementation, operation or maintenance of Transport for London (TfL) branded web sites and services; to include any site or service where there is an implicit or explicit expectation on behalf of the customer that their data is being transferred to TfL.

Requirements

1. All reasonable efforts must be made to ensure that TfL sites and services are as secure as possible
2. Security compliance takes precedence over all other requirements for any site or service
3. Penetration testing must be carries out by a reputable third party and use CVSS-SIG (Common Vulnerability Scoring System (CVSS-SIG)) because this provides an open and standardised way for rating vulnerabilities
4. All vulnerabilities rated Critical or High must be fixed
5. All vulnerabilities rated Medium or Low must be either fixed or given explicit dispensation by TfL
6. After launch, all new sites and services must be regularly tested in our Managed Security Service at a frequency that matches the site or service's security risk profile assessment, as rated by TfL

Although any reputable third party testing organisation approved by TfL can be used by you to deliver security vulnerability reports, we recommend using the company we have already engaged to deliver our Managed Security Service because this provides continuity between development and delivery and also provides a consistent framework of standards. For further detail about what testing must cover, please see our Penetration testing standard.

Why we do this

- To maintain the trust of our customers
- To protect the confidentiality of our customers
- To protect the availability of our services
- To prevent defacement of our web sites
- To protect the reputation of TfL

Further reading

Common Vulnerability Scoring System (CVSS-SIG)

Link to the toolkit's Penetration testing standard

OWASP (Open Web Application Security Project)

Type:	Guideline
Owner:	TfL Online Compliance
Department:	TfL Online

Version History

Version	Date	Summary of changes
1.0	03/06/2015	First version
2.0	10/06/2015	Updated document metadata and filename

Review History

Name	Title	Date	Comments