ვებ-გვერდის უსაფრთხოების პოლიტიკა

საქართველოს ტექნიკური უნივერსიტეტის ვებ სივრცეში არსებული ვებ-გვერდები უნდა აკმაყოფილებდნენ ქვემოთ მოცემულ წესებსა და სტანდარტებს, რომლებიც შემუშავებულია სტუ-ს კომპიუტერული ქსელის მართვის ცენტრის მიერ საერთაშორისო სტანდარტებზე დაყრდნობით.
იმისათვის, რომ ვებ-გვერდი განთავსდეს სტუ-ს ვებ-სივრცეში, იგი უნდა აკმაყოფილებდეს შემდეგ სტანდარტებს:

1. ვებ-გვერდს უნდა შეეძლოს კიბერ-შეტევების დაფიქსირება (IDS)
2. ვებ-გვერდს უნდა ქონდეს ფაიერვოლი და შეტევების მოგერიების სისტემა (Web Application Firewall & WIPS)
3. ვებ-გვერდი უნდა იყოს მდგრადი მოცემული კიბერ-შეტევების მიმართ: Sql Injection, Cross site Scripting, PHP Injections, Cross site Request Forgery, Session Hijacking, HTTP Response Splitting, Remote/Local File Inclusion, Directory Transversal, Insecure Direct Object References, Security Misconfiguration, Unvalidated Redirects and Forwards, Blind SQL Injection, Prevent Password Brute Force, BOT PROTECTION და სხვ.)
4. ვებ-გვერდმა ტექნიკური შემოწმება წარმატებით უნდა გაიაროს Acunetix Web Vulnerability Scanner-ისა და Netsparker-ის გამოყენებით ჩატარებული ტესტირებისას.

თუ ვებ-გვერდი ვერ აკმაყოფილებს მოცემულ სტანდარტებს, მაშინ ვებ-გვერდი ვერ მიიღებს სტუ-ს ჰოსტინგს, სტუ-ს ქვედომენს და მისი ბმული ვერ განთავსდება სტუ-ს საიტზე.