

מסמך דרישות חובה ממזמיני פיתוח אתרים וממפתחי אתרים עבור הטכניון - מ.ט.ל. ומוסד הטכניון למו"פ בע"מ

1 כללי

- 1.1 מטרת מסמך דרישות זה היא להסדיר את נושא פיתוח אתרי האינטרנט בטכניון ועבור הטכניון או מוסד הטכניון למו"פ בע"מ.
- 1.2 המסמך מיועד הן לספק (מפתח האתרים) והן ליחידה/הפקולטה הטכניונית המזמינה והם נדרשים לחתום על המסמך בסופו כראייה לעמידה בדרישות המסמך.
- 1.3 תוכן המסמך מחייב:
 - 1.3.1 כול אתר אינטרנט הנושא את הסיפא technion.ac.il ו- trdf.co.il בין אם האתר מתארח בחוות השרתים בטכניון או במקום אחר.
 - 1.3.2 כל אתר אשר מציג זיקה ברורה לטכניון (ברמת השימוש בלוגו ותוכן) גם אם נושא סיפא אחרת ולא מתארח בחוות השרתים של הטכניון.
 - 1.3.3 על אף האמור לעיל, מפתחי אתרים שזכו במכרז האחרון ינהגו לפי תנאי המכרז, תוך דגש על קיום הנחיות ממונה אבטחת המידע הטכניוני, אחראי ההנגשה הטכניוני, וה-DPO הטכניוני, ככל שיועברו אליהם.
 - 1.3.4 פעולות תחזוקה המתבצעות באתרים קיימים אשר הוקמו לפני חודש אפריל 2022 שהיקפן המצטבר השנתי אינו עולה על 7% מעלות הקמת האתר גם כן יהיו פטורות מהחלתם של כללים אלו.
- 1.4 כל חריגה מסעיף 1.3 דורשת אישור בכתב של סגן המשנה לנשיא למחשוב ומערכות מידע.

2 דרישות תשתית

- 2.1 שרת מארח יפעל תחת גרסה נתמכת ומעודכנת של מערכת ההפעלה, תשתיות פיתוח ומסד הנתונים.
- 2.2 על הספק לוודא קיום כול עדכוני המערכת ותוכנה בשוטף תוך 30 ימים מהכרזתם למעט עדכוני אבטחה קריטיים שיש להתקין במיידית.
- 2.3 האתר חייב להתארח ב-DMZ (בין שממומש ע"י אגף מחשוב ובין ע"י אחת הפקולטות) או מחוץ לרשת הטכניונית.

3 פיתוח ותפעול

- 3.1 הספק אחראי לתחזק את כל גרסאות הקוד בשרת GitLAB המרכזי של הטכניון, וזאת על מנת לאפשר את סריקת קוד המקור למטרות אבטחת מידע.
- 3.2 על הספק לנהל את המעבר מפיתוח לייצור באמצעות מנגנון/כלי CI/CD המאושר ע"י אגף המחשוב.
- 3.3 הספק יהיה אחראי על גיבוי מערכת הקבצים ומסדי הנתונים לפי משטר גיבויים מוסכם עם הלקוח.
- 3.4 מערכת ניהול התוכן וכלי הפיתוח יהיו מעודכנים לגרסה האחרונה או לפני האחרונה.
- 3.5 הספק אחראי למחיקה שוטפת של אובייקטים שלא בשימוש לרבות חשבונות משתמשים/תבניות/תיקיות/קבצים/תוספים וכו'.
- 3.6 מסירת האתר ללקוח תלויה במסמך בדיקות מסירה.

- 3.7 באחריות הלקוח לבצע בדיקות קבלה ולקבל אישור CISO לעלייה לאוויר לאחר סריקה וסבב תיקונים אם יידרש. אין לעלות לאוויר לפני קבלת אישור מ - CISO.
- 3.8 בכול הנושאים האחרים בתחום פיתוח ותפעול הספק מתחייב לפעול בהתאם להנחיות מנהל מחלקת פיתוח תוכנה בטכניון.

4 נגישות האתר לבעלי מוגבלויות

- 4.1 באחריות הספק בעת מסירתו להנגיש את האתר לאנשים בעלי מוגבלויות כפי המתחייב מתקנות נגישות השירות במדינת ישראל באותה עת.
- 4.2 באחריות הלקוח לוודא את נושא הנגישות בקבלת האתר והן לקיים את הנחיות הנגישות בעת הזנת התוכן.
- 4.3 הספק מתחייב למלא את הנחיות הממונה על נגישות אתרי אינטרנט בטכניון.
- 4.4 באחריות הספק והלקוח לוודא שגם כל המסמכים הנמצאים באתר מוגשים, למעט אלו הפטורים מחובת ההנגשה ע"פ החוק והתקנות.

5 אבטחת מידע

- 5.1 הגישה לאתר תותר ב - HTTPS בלבד.
- 5.2 הנפקה וחיידוש של תעודת SSL באחריות הספק מול גורם טכניוני מוסמך.
- 5.3 האתר חייב להיות מוגן ב-WAF. בהיעדר נגישות ל - WAF מרכזי הספק יעשה שימוש בתוסף WAF של מערכת ניהול התוכן.
- 5.4 גישה לכלי ניהול המערכת תוגן בפני brute force ותוגבל ברמת רשת.
- 5.5 כל המשתמשים במערכת ישתמשו בסיסמאות חזקות עם MFA.
- 5.6 בקורות אירוע אבטחת מידע - הספק יאפשר גישה לשרת המארח למטרות תחקור ופורזניקה.
- 5.7 הספק מתחייב לפעול בהתאם להנחיות הממונה על אבטחת המידע בטכניון.

6 הגנת הפרטיות

- 6.1 הספק יעשה שימוש במידע הנאסף או מעובד באתר אך ורק לצורך מתן השירותים ולא לשום מטרה אחרת.
- 6.2 ככל שהספק מספק גם שירותי אחסון, מתחייב הספק שלא להעביר את המידע לצדדים שלישיים ללא אישור בכתב מאת ה-DPO והממונה על אבטחת מידע הטכניונים.
- 6.3 על הספק להחיל מדיניות פרטיות בהתאם לדרישות הרגולציה הרלוונטית. בכל מקום באתר בו נאסף מידע פרטי, יכיל האתר הפניה למדיניות הפרטיות, ובמקרה של איסוף מידע רגיש יכלול האתר הודעה מתאימה וטופס הסכמה מדעת.
- 6.4 הספק יוודא שלא נאסף או מעובד באתר מידע שלא הוגדר ע"י הלקוח מפורשות שיש לאסוף.
- 6.5 על הספק לספק מנגנון לעדכון נתונים אישיים שגויים או לא מעודכנים.
- 6.6 על הספק לאפשר הגדרת תקופת זמן בהתאם להגדרות הלקוח להחזקת מידע על אדם שלאחריה המידע ימחק מכל המערכות בהן הוא מוחזק, לרבות גיבויים.
- 6.7 על הספק לוודא שקיימים מערכות אבטחה והצפנות אשר יגנו על המידע הפרטי באתר, כולל אפשרות למנגנון הזדהות כפולה.
- 6.8 במקרה של אירוע אבטחת מידע כהגדרתו בד"ן, יעדכן הספק את הלקוח באופן מיידי.

- 6.9 אם הספק עושה שימוש בשירותי צד ג' באתר, לרבות Cookies, יודא הספק את עמידתם בדרישות הדין בהיבטי הגנת הפרטיות.
- 6.10 הספק מתחייב לפעול בהתאם להנחיות ה - DPO בטכניון.

7 שונות

- 7.1 באחריות המשותפת של הלקוח והספק לוודא קיום הסכם תחזוקה בתוקף למשך כל התקופה בה האתר זמין באינטרנט (כולל רק ברשת הפנימית של הטכניון).
- 7.2 כל חריגה מהדרישות בסעיפים 2 עד סעיף 6 (כולל) דורשת אישור בכתב של הממונה על אבטחת המידע הטכניוני.
- 7.3 כל תשלום שיבוצע לספק יהיה מותנה בעמידתו בדרישות אלו.

שים לב: מסמך זה מתעדכן בשוטף ומה שקובע זו הגרסה המעודכנת שלו באתר cis.technion.ac.il הנושאת את חותמת הזמן האחרונה.

חתימת נציג מוסמך של היחידה המזמינה

חתימת הספק