מספר הנחיה: 2.01	שם הנחיה: נספח אבטחת מידע למכרז אתר אינטרנט אצל ספק חיצוני.
בתוקף: 15.10.2020	תאריך עדכון אחרון:14.04.2024
עורך: איתמר אופיר, ראש תחום סייבר	גרסה: 2.1

TLP: -ירוק -

נספח אבטחת מידע

מכרז אתר אינטרנט אצל ספק חיצוני

1. מטרת המסמך

מתן דגשים ודרישות בנושאי אבטחת מידע והגנת הפרטיות, עבור פיתוח אתר \ מערכת אצל ספק חיצוני.

2. איומים

האיומים המרכזיים כיום אותם יש לקחת בחשבון:

2.1. השחתת אתר אינטרנט - תקיפה של אתר אינטרנט שמטרתה, על פי רוב, היא החלפת דף הבית של האתר. השחתת האתר יכולה להיעשות רק בהינתן ההרשאות המתאימות לשינוי תוכן האתר או הרשאות המושגות במרבית המקרים על ידי ניצול פרצת אבטחה באתר עצמו או בשרת המריץ אותו.(יכול לפגוע בתדמית המשרד והמדינה).

2.2. פגיעה בסודיות – חשיפת מידע חיוני על ידי גורמים לא מורשים.

2.3. פגיעה באמינות – גרימת נזק לשלמות המידע.

2.4. פגיעה בזמינות – פגיעה במידע והשירותים הנדרשים.

3. הנחיות כלליות

3.1. על האגף האחראי במשרד על המכרז לאפיין את סוגי הנתונים (שם פרטי, ת.ז וכו') שישמרו במערכת בטרם הגשת המכרז ולהציגם לאישור אגף הביטחון.

3.2. על האתר לקבל אישור מפורש ממערכות מידע בטרם הגעתו לבדיקת אבטחת מידע.

3.3. מומלץ לערב את אגף הביטחון מתחילת התהליך, כתיבת המכרז ואפיון האתר על מנת שיחסך בזבוז זמן מיותר בהמשך הדרך.

3.4. אתר אינטרנט משרדי מחוייב להיות בעל דומיין most.gov.il אותו יש לקבל רק לאחר אישור מאגף הביטחון ואגף מערכות מידע.

3.5. על האתר להתארח אך ורק בממש"ז (ממשל זמין) – ע"פ כל אחד מהאפשרויות הבאות :

מספר הנחיה: 2.01	שם הנחיה: נספח אבטחת מידע למכרז אתר אינטרנט אצל ספק חיצוני.
בתוקף: 15.10.2020	תאריך עדכון אחרון:14.04.2024
עורך: איתמר אופיר, ראש תחום סייבר	גרסה: 2.1

TLP: -ירוק -

3.5.1. Mini-site – אתרים תדמיתיים קטנים.

3.5.2. אירוח מלא.

3.5.3. GOV אחוד - לאתר המשרדי.

3.6. בכל מקרה שאינו מאפשר לפתח באחד מהתשתיות המפורטות בסעיף 3.1 יש לקבל אישור חריג שייבחן ע"י אגף מערכות מידע ואגף הביטחון ויאושר רק במקרים חריגים מאוד.

3.7. על הספק קיימת חובת עמידה מלאה בנספח אבטחת המידע של ממש"ז (לוודא שעדכני מול מערכות מידע), במידה וישנה סתירה בנושא מסויים בין נספח אבטחת המידע של ממש"ז לבין הנספח המשרדי יש לפעול ע"פ הנספח של ממש"ז או לשאול את אגף הביטחון.

3.8. יש להחזיר למשרד את מסמך העזר מלא ע"י הספק שמתחרה במכרז לפני זכייתו, בחירת הספק הזוכה תעשה אך ורק לאחר אישור תנאי הסף של נספח אבטחת המידע. – טבלת נספח אבטחת מידע לאתר אינטרנט אצל ספק חיצוני.

3.9. יש לעבוד ע"פ הנחיות מערך הסייבר בכל הנוגע לפיתוח מאובטח, תורת ההגנה ועמידה בנהלי אבטחת המידע העדכניים כדוגמת:

3.9.1. https://www.gov.il/he/departments/general/securedevelopment

3.9.2. https://www.gov.il/he/departments/policies/cyber_security_methodology_for_organizations

3.9.3. https://www.gov.il/he/departments/topics/bp/govil-landing-page

3.10. לאחר הזכייה על הספק למלא במערכת יוב"ל (או בצורה ידנית מול אגף הביטחון) https://www.gov.il/he/departments/guides/yuvalrisk טופס הצהרה בהתאם להחלטת המשרד לגבי רמת הסיווג של הספק (ניתן ליצור קשר עם אגף הביטחון החירום והסייבר של המשרד) ולשלוח למשרד את טופס ההצהרה חתום למשרד לאישור אגף הביטחון החירום והסייבר טרם פרסום השירות \ האתר.

3.11. חובת עמידת הספק בתקן ISO27001 והצגתו למשרד טרם הזכייה במכרז, ובכל שרשרת האספקה והפיתוח בנושאי פיתוח ותחזוקת האתר.

מספר הנחיה: 2.01	שם הנחיה: נספח אבטחת מידע למכרז אתר אינטרנט אצל ספק חיצוני.
בתוקף: 15.10.2020	תאריך עדכון אחרון:14.04.2024
עורך: איתמר אופיר, ראש תחום סייבר	גרסה: 2.1

TLP: -ירוק -

4. טכנולוגי

4.1. יש לאשר מול אגף הביטחון ואגף מערכות מידע את הפלטפורמה \ השפה שבה יפותח האתר, אין להקים אתר עבור המשרד המבוסס על מערכת wordpress או כל פלטפורמה אחרת אשר המשרד .

4.2. כל העלאה של קבצים תוגבל אך ורק לסוג הקבצים הרלוונטיים (כדוגמת JPEG\PDF) , ובנוסף על כל קובץ שעולה יש לעבור מערכת SNADBOX מסודרת (חלק מנספח ממש"ז).

4.3. יש לבצע הליך אימות נתונים מחמיר לכלל שדות הקלט שבמערכת.

4.4. יש לפעול למניעת סוגי מתקפות הנמצאות ברמת הקוד בדגש על OWASP TOP 10 המעודכנות:

https://owasp.org/www-project-top-ten/

4.5. בדיקות חוסן :

4.5.1.פרסום האתר (במידה ומדובר באתר קיים יש לשלוח את הבקרות האחרונות הרלוונטיות שבוצעו) אך ורק לאחר אישור המשרד עבור המצאת בדיקות חוסן ידניות ברמתblack ו- gray box תקינות ומקיפות המאשרות את אבטחת המידע בהליך הפיתוח ובאתר עצמו.

4.5.2.יש לבצע אחת ל18 חודשים בדיקת חוסן ולעדכן את המשרד בתוצאות הבדיקה וסטטוס הפערים במידה ונתגלו כאלו באופן מידי לפני ואחרי הטיפול בהם

4.6. הספק יתחזק את סביבת הפיתוח (DEV&TEST) שאצלו בצורה מאובטחת וע"פ ההנחיות, וימנע כל פגיעה ודליפה של הקוד.

4.7. הספק ינהל ויכיר היטב ע"י בדיקה ידנית ובאמצעות מוצר המיועד לכך בסריקה של ככל הספריות, כולל תת ספריות (קוד פתוח) שבהם משתמש הספק לכתיבת הקוד, וידאג לבדוק אותם אחת לחציון שאכן אין כל בעיית אבטחת מידע בשימוש בהם.

4.8. הצפנה:

4.8.1.יש לבצע הצפנה על כלל המידע והתהליכים במנוחה ובתנועה.

4.8.2.יש לשמור הן על סודיות אלגוריתם ההצפנה והן על סודיות המַ פְ תֵ חַ . יש להקפיד על תכנון אופן שמירת המפתחות והגנת הגישה אליהם.

4.8.3.בביצוע הצפנת מידע רגיש, יש לממש אלגוריתמי הצפנה מוכרים ע"פ הכללים הבאים:

AESעבור הצפנה סימטרית

מספר הנחיה: 2.01	שם הנחיה: נספח אבטחת מידע למכרז אתר אינטרנט אצל ספק חיצוני.
בתוקף: 15.10.2020	תאריך עדכון אחרון:14.04.2024
עורך: איתמר אופיר, ראש תחום סייבר	גרסה: 2.1

TLP: -ירוק -

RSA עבור הצפנה א-סימטרית

SHA256 עבור HASH חד כיווני

4.8.4. יש להצפין את תווך הגישה באמצעות פרוטוקול TLS 1.2 ומעלה.

4.8.5. יש להשתמש בתעודה דיגיטלית המונפקת ע"י CA מוכר ומהימן.

4.8.6. מפתחות ההצפנה לא יהיו Hardcoded בקוד המקור וישמרו במקום שאינו נגיש למשתמשים.

4.9. יש לבצע עדכון PATCHES ועדכונים קריטיים בכלל המערכות הרלוונטיות באופן ישיר ועקיף לאתר.

5. אימות משתמשים

5.1. אימות אזרחים (שירות לאזרח עצמו) יתבצע אך ורק על ידי מערכת הזדהות ממשלתית (דרך ממש"ז) יש לתכנן זאת נכון ברמת הקוד בתיאום מול ממש"ז.

5.2. כל אימות של משתמש אחר (לא כשירות לאזרח עצמו) יתבצע לפחות ע"פ 2FA (אימות כפול) עם מנגנון OTP מסודר, ומנגנון כדוגמת recapcha למניעת הצפה וכו'

5.3. על האגף האחראי במשרד על המכרז לעדכן את אגף הביטחון מי האחראי הבלעדי מטעם המשרד לניהול הרשאות ע"פ נוהל כתוב מראש כולל רישום של מבקש ההרשאה וסטטוס הבקשה.

5.4. יש לאשר מול אגף הביטחון את אפיון ורמת ההרשאות לפני פיתוח המערכת.

5.5. יש לבצע בקרת גישה ורישום לוגים על כלל הפעולות והגישות באתר.

5.6. יש להציג נספח שעליו חותמים משתמשים עם חיבור \ הרשמה לאתר.

5.7. יש לנהל בצורה מרכזית את ניהול המשתמשים ואת ההרשאות שלהם ע"י גורם משרדי וע"פ נוהל שיוצגו ויאושרו קודם לכן מול אגף הביטחון.

5.8. כל פרסום מידע באתר חייב להיות באישור, בקרה ופיקוח של אגף הביטחון והמחלקה המשפטית.

6. הצגת אפיון תואם

לאחר הזכייה ובטרם העלאת האתר, על הספק לתאר ולצרף מסמך המתאר את מדיניות אבטחת המידע של השירות המוצע לאגף הביטחון ולאגף מערכות מידע.

מספר הנחיה: 2.01	שם הנחיה: נספח אבטחת מידע למכרז אתר אינטרנט אצל ספק חיצוני.
בתוקף: 15.10.2020	תאריך עדכון אחרון:14.04.2024
עורך: איתמר אופיר, ראש תחום סייבר	גרסה: 2.1

TLP: -ירוק -

הפירוט יכלול בין היתר את הנושאים הבאים:

6.1. נוהל ניהול משתמשים והרשאות באתר.

6.2. תיאור ארכיטקטורה של המערכת המוצעת.

6.3. רשימת ספריות הקוד הפתוח.

6.4. שפת התכנות \ הפלטפורמה עליה מושתת האתר.

6.5. בקרות אבטחת המידע אשר בשימוש המערכת.

6.6. נהלי גיבוי ו-DR.

6.7. אופן שילוב תהליך SDLC במחזור חיי המערכת.

6.8. תהליכים ארגוניים לצמצום סיכונים והתמודדות עם איומים.

6.9. המצאות והערכה של תאימות לתקינה ולחוקים.

6.10. אופן זיהוי ותגובה לאירועים.

6.11. הערכת עובדים ובדיקות מהימנות.

6.12. ביצוע מבדקי חדירה תקופתיים.

6.13. יישום מנגנוני ניטור ובקרה.

6.14. אופן הטיפול בנושא הזדהות וניהול הרשאות.

6.15. זיהוי חולשות והתקנת טלאים.

6.16. במידה וספק המערכת מבצע שימוש בתשתית מחשוב של ספק אחר, עליו לציין זאת ולצרף מסמך המתאר כיצד מתבצעת חלוקת האחריות בינו לבין ספק התשתית הנוסף ובאילו אמצעים הוא נוקט בכדי להגן על המידע מפני פגיעות ברמת התשתית.

7. הגנת הפרטיות

7.1. במידה והאתר מכיל "מאגר נתונים" (ע"פ הגדרת הרשות להגנת הפרטיות וע"פ שיקול אגף הביטחון) טרם איסוף הנתונים ושמירתם יש לשלוח לאגף הביטחון החירום והסייבר ולמחלקה המשפטית במשרד אישור של רישום המאגר במשרד המשפטים.

7.1.1.הספק מתחייב לעמוד בהוראות חוק המחשבים , התשנ"ה 1995 – דיני הגנת הפרטיות ובכללם חוק הגנת הפרטיות , התשמ"א , 1981 ותקנות הגנת הפרטיות

מספר הנחיה: 2.01	שם הנחיה: נספח אבטחת מידע למכרז אתר אינטרנט אצל ספק חיצוני.
בתוקף: 15.10.2020	תאריך עדכון אחרון:14.04.2024
עורך: איתמר אופיר, ראש תחום סייבר	גרסה: 2.1

TLP: -ירוק -

(אבטחת מידע) התשע"ז 2017.

7.1.2.בכל אסיפת מידע נוסף שלא תוכלל בתחילת הפרויקט יש לעבור אישור מחודש מול המחלק המשפטית ואגף הביטחון

7.1.3.הספק ידאג לאבטחת כל חומר שיגיע אליו במסגרת ביצוע התחייבויותיו על פי הסכם זה ויהיה אחראי כלפי המשרד על כל המידע המועבר אליו או דרכו לרבות דוחות, נתונים אישיים, תכתובות דוא"ל, קבצים, מסמכים, שרטוטים וכיו"ב על פי ההנחיות שיועברו על ידי המשרד.

7.1.4.באחריות הספק לדאוג לחיסיון, אמינות וזמינות המידע של המשרד שברשותו.

7.1.5.מידע רגיש של המשרד , המסומן בסיווג "מוגבל" ו/או "חסוי" ו/או "אישי" (להלן "מידע מוגבל") המועבר בין המשרד והספק בצורה מקוונת /דיגיטלית ,יהיה בפורמט שאינו מאפשר את עריכתו כגון (PDF מוגן משינויים /עריכה) וישמר אצל הספק בתצורה זאת .

7.2. ככל שהמסמך יועבר מוצפן , הרי שהמסמך יישמר אצל הספק בתצורה מוצפנת.

7.3. אין להסיר ממסמכי המשרד המגיעים לספק את סימון המידע "מוגבל/חסוי"

7.4. מידע "מוגבל" יהיה נגיש לעובדי הספק ע"פ הגדרת הצורך לדעת (Know to Need. (הכנת עותקים לצרכי עבודה אצל הספק תיעשה על פי צורך בלבד ותפוצתם תהא בקרב עובדי הספק הנדרשים לעותקים אלו בלבד.

7.5. חל איסור על הספק להעביר מידע לכל גורם אחר ללא אישור מפורש מצד המשרד.

7.6. חל איסור על הספק להעביר מידע המסומן כ"מוגבל/חסוי" לגורמי צד שלישי.

7.7. על הספק ליישם יכולת הגדרה במערכי הניטור לרישום גישה או ניסיונות גישה למידע המוגדר כרגיש.

7.8. על הספק ליישם יכולת סימון של רמות רגישות המידע בדוחות המערכת.

7.9. על הספק לדאוג לכך כי תיושם יכולת ערבול) Obfuscation)של נתונים המועברים מסביבת ה- production לסביבות אחרות.

7.10. הספק יחתום על התחייבות לשמירת סודיות, בנוסח המצורף למכרז, וכן יחתים על התחייבות זו את עובדיו ו/או כל מי מטעמו אשר יהיה בעל גישה למאגר מידע של המשרד או למידע מתוכו במסגרת ההתקשרות.

מספר הנחיה: 2.01	שם הנחיה: נספח אבטחת מידע למכרז אתר אינטרנט אצל ספק חיצוני.
בתוקף: 15.10.2020	תאריך עדכון אחרון:14.04.2024
עורך: איתמר אופיר, ראש תחום סייבר	גרסה: 2.1

TLP: -ירוק -

8. אחריות באירועי סייבר

8.1. הספק יהיה אחראי לכל עקיפה או ניסיון עקיפת מנגנוני אבטחה ובקרות גישה ברמת הקוד\תשתיות ,שיבוצע על ידי מי מהעובדים מטעמו.

8.2. הספק מתחייב לשיתוף פעולה מלא עם המשרד בכל אירוע חריג בו מעורב הספק ,או שקיים חשד למעורבות שיש עמה השלכה ישירה או עקיפה על ביטחון מערכות המידע של המשרד , בכל הפרה או חשד להפרה של חוקים תקנות או נהלי אבטחת מידע כולל בחקירת אירועים או חשדות לחריגות אבטחת מידע או דליפת מידע של המשרד לגורמים בלתי מורשים.

8.3. הספק מתחייב למנות ממונה על אבטחת המידע מטעמו, אשר יהיה אחראי על הטיפול במאגרי המידע המצויים בידי הספק וכן על יישום ההנחיות המופיעות במסמך זה וניהול אבטחת המידע בקוד ובספריות (כדוגמת קוד פתוח) בהם השתמש.

8.4. הספק לא ישמור אצלו מאגר מידע אלה אך ורק בסביבת הPRODUCTION שבממש"ז.

8.5. בכל מקרה שבו לספק התקשרות עם צד שלישי כלשהו אשר יש לה נגיעה עם ההתקשרות בין הספק למשרד במסגרת מכרז זה ו/או על יישום ההנחיות המפורטות במסמך זה, הספק מתחייב להודיע על כך למשרד ולפעול על פי הנחיותיו וכן ליידע את הצד השלישי על החובות הנובעות מקיום ההנחיות המפורטות במסמך זה.

8.6. המשרד רשאי לבצע בקרה תהליכית אצל הספק ,לאחר תיאום עמו. הספק מתחייב לשתף פעולה עם נציגי המשרד לצורך כך.

8.7. יש לחתום על מסמך התחייבות לשמירה על סודיות, (NDA) שיסופק על ידינו.

9. חובת דיווח

9.1. על כל אירוע\חשש לאירוע של אבטחת מידע \ הגנת הפרטיות הרלוונטי עבור משרד המדע התרבות והספורט יש לדווח באופן מידי לאגף הביטחון של המשרד גם במספר : 072-345-2355 וגם במייל cyber@most.gov.il.

9.2. לאחר הזכייה על הספק לפרט תכנית ביצוע לניהול וזיהוי סיכוני אבטחת מידע בכל שלב משלבי הפרויקט .

מספר הנחיה: 2.01	שם הנחיה: נספח אבטחת מידע למכרז אתר אינטרנט אצל ספק חיצוני.
בתוקף: 15.10.2020	תאריך עדכון אחרון:14.04.2024
עורך: איתמר אופיר, ראש תחום סייבר	גרסה: 2.1

TLP: -ירוק -

9.3. הספק מתחייב לפנות למשרד בבקשה לאישור לפני ביצוע שינויים בארכיטקטורת המערכת, או באופן מתן השירותים. הספק מתחייב שלא לבצע שינוי כלשהו ללא אישור מפורש ובכתב מהמשרד.

9.4. הספק רשאי להציע בקרות חלופיות לדרישות המפורטות במסמך זה, בקרות אלו ייושמו לאחר אישור בכתב של גורמי אבטחת המידע במשרד.

10. אבטחת המידע במישור משאבי האנוש והעובדים:

10.1. הספק מתחייב כי כל עובדיו ו/או מי מטעמו אשר יהיו בעלי גישה למאגרי המשרד ו/או יועסקו במסגרת התקשרות הספק עם המשרד, יהיו בעלי הכשרה מתאימה, בהתאם לנדרש במסמכי המכרז וההתקשרות. בדיקת אימות הרקע של כל מועמד להעסקה כעובד הספק, מי מטעמו או משתמש צד שלישי, יעשו ע"י הספק כנדרש על פי דין ולפי כללי האתיקה הרלוונטיים, והיקפם יתאים לדרישות המשרד, לסיווג המידע שיהיה נגיש להם ולסיכונים הצפויים.

10.2. הספק יהיה אחראי כלפי המשרד על כל פעילות עובדיו ו/או מי מטעמו במסגרת ההתקשרות.

10.3. הספק מתחייב שכל עובדיו, ו/או מי מטעמו ו/או משתמשי צד שלישי, מבינים את מלוא האחריות המוטלת עליהם בנוגע למידע ולאבטחתו וכי הם מתאימים לתפקידים שנועדו להם.

10.4. על הספק להפחית סיכוני גניבה, הונאה או שימוש לרעה בגישה למידע של המשרד באמצעות נקיטת אמצעי הגנה סבירים ומקובלים כגון מצלמות אבטחה, תיעוד גישה וכדומה, וזאת מבלי לגרוע מהוראות נספח זה באשר לאבטחה הפיזית והסביבתית.

10.5. על הספק לבצע הדרכות מודעות אבטחת מידע לעובדיו בתחום העיסוק של העובד בתדירות של אחת לשנה לכל הפחות.

10.6. הספק מתחייב למנוע מקרים בהם עובדיו ו/או מי מטעמו ינסו לבצע גישות למאגרים אליהם לא קיבלו הרשאה.

10.7. הספק מתחייב כי תפקידים ותחומי אחריות של עובדי הספק ו/או מי מטעמו ו/או משתמשי צד שלישי הנוגעים לאבטחה , יוגדרו ויתועדו ע"י הספק לפי מדיניות אבטחת המידע של הארגון.

מספר הנחיה: 2.01	שם הנחיה: נספח אבטחת מידע למכרז אתר אינטרנט אצל ספק חיצוני.
בתוקף: 15.10.2020	תאריך עדכון אחרון:14.04.2024
עורך: איתמר אופיר, ראש תחום סייבר	גרסה: 2.1

TLP: -ירוק -

10.8. חוזה הנחתם עם עובדים חדשים יכלול התייחסות לאחריות העובד בכל הנוגע להיבטי אבטחת מידע, וילווה בהצהרת סודיות.

10.9. חוזה של הספק עם חברות כוח אדם/השמה או עם חברות המספקות שירותי מיקור חוץ, יכלול התייחסות בכל הנוגע לבדיקות המבוצעות בתהליכי גיוס העובדים. אבטחת מידע בעת העסקת עובדים והגברת המודעות שלהם, נוהלי אבטחת מידע של הספק יגדירו מהן הפעולות שיש לבצע בכדי לשמור על נכסי המידע של המשרד.

10.10. על הספק להגדיר נהלים, בקרות ופעולות נוספות המיועדות למנוע את זליגת המידע מעובדים להם יש נגישות למידע של המשרד.

10.11. לעובדים (כולל עובדים חיצוניים לארגון) המסיימים את העסקתם בארגון, בין אם ביוזמתם או ביוזמת המעסיק, ייחסמו הרשאות הגישה למידע בין אם למערכות מידע ובין אם לאמצעים פיזיים.

10.12. הספק יוודא כי בסיום ההעסקה לא יישארו נכסי מידע של הארגון בידי העובד.

10.13. הספק יגדיר את אופן הטיפול בעובדים בהיבטי אבטחת מידע לתקופת הזמן שבין הודעת העזיבה לסיום העסקה. יש להגדיר דרישות לפחות בנושאי בקרת גישה, עבודה על מערכות ומסמכים וכו'.

11. אבטחת מידע פיזית וסביבתית

11.1. הספק מתחייב כי הגישה לאזורים שקיים בהם מידע ו/או מאגרי מידע וארונות התקשורת תהיה מתועדת ומבוקרת באופן המאפשר את וידוא זהות האדם הניגש לציוד הנ"ל.

11.2. בכל מקרה בו מאגר המידע נמצא ברשות הספק, הספק מתחייב לתעד הכנסה והוצאה של ציוד אל המתקנים בהם ממוקם המאגר ומהם.

11.3. הספק מתחייב כי כניסת ספקים או לקוחות לאזורי חוות השרתים תהיה מבוקרת, תכלול ליווי, ותירשם ביומן רישום אירועים.

11.4. אמצעים לבקרת כניסה פיזית: הספק מתחייב כי השרתים והציוד המשמש לאחסון , עיבוד וגישה למאגרי המידע והיישומים יוגנו על ידי אמצעים מתאימים לבקרת כניסה כדי להבטיח שרק לעובדים מורשים תותר הגישה.

11.5. הגנה מפני איומים סביבתיים: הספק מתחייב ליישם הגנה פיסית מפני נזקים של שריפה, הצפה , רעידות אדמה, פיצוצים, הפרות סדר וסוגים אחרים של אסונות טבע ופגיעות מעשה ידי אדם.

11.6. עבודה באזורים מאובטחים: הספק מתחייב לכתוב וליישם הנחיות לעבודה באזורים מאובטחים.

11.7. שירותים תומכים: הספק מתחייב להגן על הציוד בפני הפסקות חשמל והפרעות אחרות הנגרמות בגלל כשל שירותים תומכים.

11.8. אבטחת כבלים: הספק מתחייב כי כבלי חשמל ותקשורת הנושאים נתונים או תומכים בשירותי מידע, יוגנו מפני יירוט או נזק.

11.9. תחזוקת ציוד: הספק מתחייב לתחזק את הציוד כראוי על מנת להבטיח את זמינותו וכלילותו הרציפות.

12. פיתוח התוכנה

בכל הנוגע לפיתוח תכנה על הספק לעבוד ע"פ עקרונות תורת ההנגה בסייבר וע"פ מסמך פיתוח מאובטח ומסמך העזר בקישור הבא:

https://www.gov.il/he/departments/general/securedevelopment

12.1. קוד התוכנה יכיל רק את הנרשם בתיעוד המסופק עם התוכנה ואשר סוכם עם המשרד.

12.2. קוד התוכנה יהיה ללא רישום של סיסמאות ניהול, דלתות אחוריות, סוסים טרויאנים וכיו"ב.

12.3. התוכנה תיבדק ע"י בוחני איכות בתהליך Review Code בצורה מעמיקה, כולל תיקון באגים הפוגעים באבטחת המידע של המערכת.

12.4. פגיעות זו, במידה וקיימת תתוקן ודיווח על כך יועבר למשרד.

12.5. הקוד ייסרק באמצעי SAST ו-DAST. ליקויי אבטחה אשר יופיעו בדוח הסריקה יתוקנו בטרם העלאתם לסביבת הייצור.

12.6. המערכת לא תבצע שינויי קוד במערכות נלוות כגון מערכת הפעלה אשר פוגעים ברמת אבטחת המידע הכללית של מערכות המחשוב של המזמין.

מספר הנחיה: 2.01	שם הנחיה: נספח אבטחת מידע למכרז אתר אינטרנט אצל ספק חיצוני.
בתוקף: 15.10.2020	תאריך עדכון אחרון:14.04.2024
עורך: איתמר אופיר, ראש תחום סייבר	גרסה: 2.1

TLP: -ירוק -

12.7. הספק מתחייב כי בגרסאות עתידיות של המערכת לא יתבצעו שינויים מהותיים, להבדיל מבאגים לא צפויים, אשר יפגעו ברמת אבטחת ללא תיאום ואישור בכתב מהמשרד.

13. גיבוי,שחזור והתאוששות

13.1. מידע של המשרד, הנמצא במערכות הספק יגובה בצורה סדירה. על פי המדיניות שיקבע המשרד.

13.2. הספק מתחייב לבצע גיבויים מאובטחים ומוצפנים של המידע הנצבר אצלו.

13.3. הספק מתחייב לאחסן את מדיות הגיבוי בכספת מוגנת אש ומים הנמצאת מחוץ למתקן המחזיק את מאגרי המידע או שהספק יעשה שימוש באמצעים שיבטיחו את שלמות המידע ויבטיחו את אפשרות שחזור המידע במקרה של אבדן או הרס.

13.4. הספק מתחייב לבצע שחזורים מדגמיים של המדיות המגבות על תשתיותיו לצורך בדיקת התאוששות.

13.5. לאחר סיום השחזור המדגמי מתחייב הספק למחוק את המידע ששוחזר.

13.6. הספק מתחייב כי שחזור אמתי יבוצע אך ורק באישור אגף הביטחון.

13.7. הספק מתחייב כי במידה ובוצע שחזור אמתי יתועדו כל הליכי השחזור כולל זהותו של מבצע השחזור.

13.8. הספק מתחייב למנוע עירוב מידע מסיווגים שונים בזמן השחזור.

14. סיום התקשרות

14.1. הקוד שייכתב במסגרת המכרז יהיה בבעלות של משרד המדע התרבות והספורט, ובכל סיבה בה יוחלט לנתק קשר עם הספק יועבר הקוד בצורה מלאה לידי המשרד בצורה מאובטחת ותקינה.

14.2. המשרד ידרוש מהספק את מחיקת המידע בסיום ההתקשרות, או בכל נקודת זמן שקודמת לה (לדוגמה במקרה של חשד לפריצה ו/או דלף מידע אצל הספק), על הספק לבצע בעת סיום ההתקשרות מחיקה מלאה של הנתונים (גם בגיבויים ומקומות נוספים בהם נשמר המידע).

14.3. יש לוודא כי הסדרים עם הספק שנקבעו במסגרת הסכם ההתקשרות, מתקיימים. בפרט חשוב לוודא עמידה בכל הקשור למחיקת נתונים של הארגון המאוחסנים בחצרי הספק בתום ההתקשרות בין הצדדים.

בין היתר יש לבדוק את הנושאים הבאים:

14.3.1. - יש לוודא החזרת כלל הרשומות, המדיה, הציוד והרכיבים השייכים לארגון אשר נעשה בהם שימוש לצורך עבודת הספק. כל זאת, לרבות פריטים הנמצאים בקרבכלל עובדי הספק וספקי המשנה שלו.

14.3.2. הספק יחתום על הצהרה בה הוא מתחייב שלא נשארו ברשותו רכיבים כלשהם הנוגעים למערכת ו/או מידע אודות הארגון וכי הוא לא יעשה שום שימוש במידע על הארגון, אליו הוא נחשף במסגרת ההתקשרות.

14.3.3. יש לוודא השמדת מדיה מגנטית מכל ציוד אשר שימש את הספק במהלך ההתקשרות עם הארגון (כגון: במקרה שמדובר במחשבים של הספק ששימשו לעיבוד ו/אחסון של מידע של הארגון).

14.3.4. כמו כן, נדרש לוודא מחיקת עותקים של קבצים ומידע של הלקוח ממערכות המידע ונכסי ה-IT של הספקים לאחר סיום הצורך העסקי באחזקתו.

14.4. יש לוודא כי לספק לא נותרות הרשאות גישה, אמצעי הזדהות וגישה פיזית ו/או לוגית למידע של הארגון.

14.5. יש לוודא הנחיה לעניין המותר והאסור אודות פרסום פרטי הפרויקט/התקשרות לגורמי צד ג'.