נספח אבטחת מידע

מכרז אתר אינטרנט אצל ספק חיצוני

1. מטרת המסמך

מתן דגשים ודרישות בנושאי אבטחת מידע והגנת הפרטיות, עבור 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. כללי

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

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

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

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

3.2. על הספק למלא במערכת יוב"ל 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.

3.3. אחסון אתר ממשלתי יהיה אך ורק בשרתי ממש"ז או לחלופין בשרתי המשרד באישור אגף הביטחון ומערכות מידע כל זאת בהלימה להחלטת ממשלה 2097.

3.4. עמידה הספק בתקן ISO27001 והצגתו למשרד טרם פרסום האתר, ובכל שרשרת האספקה והפיתוח בנושאי פיתוח ותחזוקת האתר.

3.5. בדיקת חוסן :

3.5.1. פרסום האתר (במידה ומדובר באתר קיים יש לשלוח את הבקרות האחרונות הרלוונטיות שבוצעו) אך ורק לאחר אישור המשרד עבור המצאת בדיקת חוסן תקינה המאשרת את אבטחת המידע בהליך הפיתוח ובאתר עצמו.

3.5.2. יש לבצע אחת ל18 חודשים בדיקת חוסן ולעדכן את המשרד בתוצאות הבדיקה וסטטוס הפערים במידה ונתגלו כאלו.

3.6. הצפנה

3.6.1. יש לבצע הצפנה על כלל המידע והתהליכים הרגישים.

3.6.2. יש להצפין את תווך הגישה באמצעות פרוטוקול TLS.

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

3.7. אימות משתמש יתבצע לפחות ע"פ 2FA (אימות כפול), מנגנון כדוגמת recapcha למניעת הצפה וכו'

3.7.1. במידה ומדובר על מערכת ממשלתית אך ורק האימות התבצע אך ורק ע"י מערכת הזדהות אחודה של ממשל זמין ותיאום מלא מול אגף מערכות המידע של המשרד. וכל זאת בהתאמה וע"פ החלטת ממשלה 2960.

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

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

3.10. על הספק להציג תעודה שהוא עומד בתנאי שרשרת האספקה או לחלופין למלא שאלון שרשרת אספקה בליווי המשרד.

4. הצגת אפיון תואם

על הספק לתאר ולצרף מסמך המתאר את מדיניות אבטחת המידע של השירות המוצע.

הפירוט יכלול:

4.1. תיאור ארכיטקטורה של המערכת המוצעת.

4.2. בקרות אבטחת המידע אשר בשימוש המערכת.

4.3. נהלי גיבוי ו-DR.

4.4. אופן שילוב תהליך SDLC במחזור חיי המערכת.

4.5. תהליכים ארגוניים לצמצום סיכונים והתמודדות עם איומים.

4.6. המצאות והערכה של תאימות לתקינה ולחוקים.

4.7. אופן זיהוי ותגובה לאירועים.

4.8. הערכת עובדים ובדיקות מהימנות.

4.9. ביצוע מבדקי חדירה תקופתיים.

4.10. יישום מנגנוני ניטור ובקרה.

4.11. אופן הטיפול בנושא הזדהות וניהול הרשאות.

4.12. זיהוי חולשות והתקנת טלאים.

4.13. 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.

5. הגנת הפרטיות

5.1. טרם איסוף הנתונים ושמירתם יש לשלוח לאגף הביטחון החירום והסייבר ולמחלקה המשפטית במשרד אישור של רישום המאגר במשרד המשפטים.

5.2. הספק מתחייב לעמוד בהוראות חוק המחשבים , התשנ"ה 1995 – דיני הגנת הפרטיות ובכללם חוק הגנת הפרטיות , התשמ"א , 1981 ותקנות הגנת הפרטיות (אבטחת מידע) התשע"ז 2017.

5.3. הספק מתחייב למלא אחר כל הוראות אבטחת המידע לגבי שמירת מידע כפי שיועברו ע"י המשרד.

5.4. 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.

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

5.6. הספק יהיה אחראי לכל עקיפה או ניסיון עקיפת מנגנוני אבטחה ובקרות גישה לתשתיות שונות ,שיבוצע על ידי מי מהעובדים מטעמו.
בעת אירוע אבטחת מידע או אירוע חריג אצל הספק ,בו קיים חשד לגבי דלף מידע של המשרד, הספק מחויב להודיע באופן מידי לאיש הקשר מטעם המשרד.

5.7. הספק מתחייב לשתף פעולה עם המשרד בכל אירוע חריג בו מעורב עובד 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.

5.8. מידע רגיש של המשרד , המסומן בסיווג "מוגבל" ו/או "חסוי" (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 . ככל שהמסמך יועבר מוצפן , הרי שהמסמך יישמר אצל הספק בתצורה מוצפנת.

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

5.10. המגיע מהמשרד.

5.11. מידע "מוגבל" יהיה נגיש לעובדי הספק ע"פ הגדרת הצורך לדעת (Know to Need.)

5.12. הכנת עותקים לצרכי עבודה אצל הספק תיעשה על פי צורך בלבד ותפוצתם תהא

5.13. בקרב עובדי הספק הנדרשים לעותקים אלו בלבד.

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

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

5.16. על הספק ליישם יכולת הגדרה במערכי הניטור לרישום גישה או ניסיונות גישה

5.17. למידע המוגדר כרגיש.

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

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

5.20. 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.

5.21. 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.

5.22. הספק מתחייב להפריד הפרדה מלאה את מאגרי המשרד המצויים בידיו מיתר מאגרי המידע שברשותו.

5.23. 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.

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

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

5.26. יש לרשום את המאגר בצורה המקובלת, תוך כידי עמידה בתנאי משרד המשפטים בכל הנוגע לתחום הגנת הפרטיות.

6. חובת דיווח

על כל אירוע של אבטחת מידע \ הגנת הפרטיות הרלוונטי עבור משרד המדע התרבות והספורט יש לדווח באופן מידי לאגף הביטחון של המשרד.

6.1. על הספק לפרט תכנית ביצוע לניהול וזיהוי סיכוני אבטחת מידע בכל שלב משלבי הפרויקט .

6.2. 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.

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

7. אבטחת המידע במישור משאבי האנוש והעובדים:

7.1. 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.

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

7.3. 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.

7.4. 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.

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

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

7.7. 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.

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

7.9. 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.

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

7.11. 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.

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

7.13. 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'.

8. אבטחת מידע פיזית וסביבתית

8.1. 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.

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

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

8.4. 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.

8.5. 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.

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

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

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

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

9. פיתוח התוכנה

בכל הנוגע לפיתוח תכנה על הספק לעמוד בהנחיית יה"ב 10.5 – בנושא פיתוח מאובטח. בנוסף, על הספק ליישם את הדגשים הבאים:

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

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

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

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

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

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

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

10. גיבוי,שחזור והתאוששות

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

10.2. הספק מתחייב לבצע גיבויים מאובטחים של המידע הנצבר אצלו.

10.3. 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.

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

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

10.6. הספק מתחייב כי שחזור אמתי יבוצע אך ורק באישור מנהל אבטחת המידע.

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

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

11. סיום התקשרות

11.1. 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).

11.2. 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:

11.2.1. - 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.

11.2.2. 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.

11.2.3. 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).

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

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

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