נספח 4 - אבטחת מידע והגנה בסייבר להקמת מתחם המשקף במעבר ניצנה

1. דרישות כלליות

1.1 הספק/הזוכה/נותן השרות – ובכלל זה ספקי המשנה וכל המעורבים בפיתוח, הקמה או תחזוקה – יעמוד בכל דרישות אבטחת המידע והגנת הסייבר בין אם ההנחיות פורטו בנספח אבטחת מידע ובין אם יועברו בהמשך לאחר קביעת הזוכה.

1.2 במסגרת המכרז, יידרש הספק לתכנן, לבנות ולתחזק סביבות מחשוב/רשתות תקשורת אקטיבית/פאסיבית כאשר סביבות אלה יתמכו את התהליכים הנדרשים לתפעול מלא של אתר המשקף של רשות המיסים – אגף המכס.

1.3 הספק ידאג כי כלל דרישות אבטחת המידע מוכלות על כלל הרכיבים לרבות מוצרי מדף שיירכשו ויוטמעו על ידו במסגרת הפרויקט. בנוסף, על הספק לדאוג לכל תהליכי אבטחת המידע במערכות שבאחריותו ובקישור למערכות אחרות בסביבות אחרות.

1.4 בכל שלבי הפרויקט, נאסר על הספק להתחבר לרשת רשות המיסים - אגף המכס, לרבות חיבור בין סביבה לרשת האינטרנט.

1.5 כלל הרשתות שיתוכננו ויבנו ע"י הספק לא יחוברו בשום תצורה לרשת האינטרנט.

1.6 בכל שלב בתכנון והקמת המערכות ועבור כל שירות/רכיב/תשתית שישתלב בפתרון יידרש אישור פרטני של תחום אבטחת מידע ברשות המיסים - אגף המכס.

1.7 על המציע לפרט את כלל היבטי הגנת הסייבר של הפתרון המוצע, ברובד הגנת המידע, הגנת המערכות והגנה על תשתיות IT ומרכיבים נוספים, ובפרט בהיבטים באים:

1.7.1 "הרעיון המסדר" ובפרט, ארכיטקטורת הגנת המידע (לרבות "מידע על המידע", קרי - מידע ניטור ובקרה), לרבות ההיבטים הבאים:

1.7.1.1 חסיון מידע העונה לדרישות החוק והפרטיות.

1.7.1.2 הגנת מידע במנוחה, בעיבוד ובתנועה.

1.7.1.3 מנגנוני זיהוי, הזדהות חזקה.

1.7.1.4 חסימה באמצעות DEVICE CONTROL

1.7.2 על המציע לתאר את מרכיבי הטופולוגיה המוצעת, חומרות, תוכנות, מסלולי זרימת מידע והקשחות

גרסא : 1.0	תאריך תחולה:	עמוד **2** מתוך **6**
נספח אבטחת מידע והגנה בסייבר להקמת מתחם משקף מעבר ניצנה	תאריך יצירה: 19.03.2023	

2. <u>דרישות לתכנון ויישום של הספק</u>

2.1 אבטחת פיזית ובטחון מידע

2.1.1 היבטי האבטחה הפיסית יוגדרו על בסיס הנחיות ממונה הביטחון של רשות המיסים - אגף המכס ומפורטות בנספח אבטחה פיזית.

2.1.2 מהימנות כ״א: כוח האדם בפרויקט, לכל אורך שלבי הפרויקט יסווג בהתאמה להנחיות ממונה הביטחון.

2.1.3 הוצאת מידע: אין להוציא חומר, קשיח או רך, הקשור בפעילות אתר השיקוף, על כל סביבותיו, מחוץ לאתר/מתקן, לרבות הדפסות של מידע מתוך הרשתות השונות שבאתר או תמונות שיקוף.

2.2 עמידה בדרישות חוק, תקנות ותקני אבטחת מידע

2.2.1 הפתרון המוצע נדרש לענות על דרישות אבטחת המידע ואחרות המפורטות בגרסתם ומהדורתם העדכנית ביותר של החוקים, התקנות, התקנים והמפרטים הבאים. יובהר כי הדרישה מהספק מתייחסת רק לתשתיות ומערכות שבאחריות הספק ולא על מערכות המזמין קרי – הסביבה המקומית של הספק (כל תשתית ה-IT שבמוקד השרות הרשותי) והתשתית שתוקם לצורך מימוש ממשקים למערכות פנימיות של רשות המיסים - אגף המכס:

2.2.1.1 הוראות כל דין המתייחס למערכות ממוחשבות, ובפרט - חוק המחשבים, התשנ״ה – 1985, חוק זכות יוצרים, התשס״ח-2007 וקניין רוחני.

2.2.1.2 חוק הגנת הפריות תשמ״א-1981 (כולל תקנות הגנת הפרטיות/תקנה 13)

2.2.1.3 מדיניות אבטחת המידע של רשות המיסים - אגף המכס.

2.3 אימות, ניהול הזהויות וההרשאות

2.3.1 על הספק לתאר את מנגנוני ההזדהות, על כלל המערכות והממשקים, שהפתרון תומך בהם, וכן הצבעה על מנגנון המימוש המתוכנן.

2.3.2 על הפתרון לתמוך במנגנון הזדהות חזקה, לכלל המערכות והתשתיות בפרויקט. יצוין כי עבור גישת משתמשים ההזדהות תתבסס על 2FA. אורך, מורכבות ותוקף הסיסמא תיקבע ע״י המזמין בשלבי תכנון הפרויקט.

2.3.3 ברשתות שבאחראיות הספק, המשתמשים ינוהלו בצורה מרכזית באמצעות ארגוני כגון: Active Directory.

2.3.4 ככל הניתן ובכל מקום שמתאפשר המערכת תתמוך ביכולת הזדהות אחודה(SSO) של המשתמש בעת ההתחברות לממשקי הניהול והמשתמש.

2.3.5 חל איסור שימוש ב- Shared Credential במערכות ההפעלה, אפליקציות, מנהלי מערכת וכו׳. המימוש יהיה באמצעות נהלים ובקרות.

2.3.6 המערכת תתמוך במנגנון הרשאות מרכזי על פי דרישות המערכת ואשר יתמוך בעקרונות הבאים:

2.3.6.1 עקרון ההרשאה המזערית: בכל מערכת ובכל רכיב מערכת יש לאפשר גישה אך ורק לגורמים מורשים ומזעריים ככל שניתן.

2.3.6.2 הגבלת הגישה למשאבי המערכת: יש להגביל אילו משתמשים יכולים לגשת למשאבים כגון: קבצים, תיקיות, registry keys, וכד'. ומה הם יכולים לבצע (קריאה, כתיבה, יצירה, הרצה ומחיקה).

2.3.6.3 הרשאות מזעריות עבור משתמש בסיס הנתונים: בגישה לבסיס הנתונים לצורך פעולות של אימות, שליפה ועדכון נתונים, יש צורך לוודא שהרשאות הן ל-Store Procedure בלבד או מזעריות ככל שניתן.

2.3.7 הפתרון יתמוך בהענקת הרשאות לצורכי הזדהות ברמת מערכת ההפעלה, רכיבי תקשורת, בסיסי נתונים ואפליקציה בהתבסס על משתמשים/קבוצות ב-AD.

2.3.8 על הספק נדרש לנעול חיבורים כתוצאה מחוסר פעילות זמני, ולא לאפשר את המשכיות החיבור עד להזדהות ואימות חוזר של המשתמש. כחלק מביצוע נעילת החיבור יש להסתיר מידע שהוצג על המסך טרם הנעילה.

2.3.9 על הספק נדרש להגביל התחברות משתמש למערכת לאחר מספר ניסיונות התחברות כושלים, באמצעות נעילת האפשרות לביצוע התחברות במשך פרק זמן מוגדר או עד לשחרור ע"י מנהל מערכת. ניתן להגביל את מספר הניסיונות הכושלים להתחברות בתוך ה Group Policy וה – Domain Policy.

2.3.10 על הספק נדרש להגביל את מספר החיבורים המותרים בו-זמנית של משתמש בודד ככל הניתן. ניתן להגביל מספר התחברויות בו זמנית בתוך מדיניות ה Logon Remote ב Group Policy.

2.4 הפרדת תשתיות פאסיביות

2.4.1 על הספק נדרש לתכנן וליישם פריסת כבלי/סיבי/ריכוזי תקשורת נפרדים עבור רשתות שונות הנפרדות פיזית בחלק האקטיבי שלהן. לדוגמא תשתיות רשת רשות המיסים – אגף המכס לא תוקמנה לעולם בריכוזי תקשורת עם רשת המשקף או רשתות אחרות.

2.4.2 על הספק לבצע הפרדה פאסיבית ובכלל זה חדרי תקשורת ומרכזי מחשוב נפרדים עבור כל אחד מהרשתות השונות.

2.5 הגנת עמדות קצה ושרתים

2.5.1 על הספק הזוכה לדאוג להקשחה של כלל המערכות שסופקו ו/או נמצאים באחריותו, כגון: Windows Server, Database, AV, Firewall ,Switch ועוד. הקשחה זו צריכה להתבסס על הנחיות Best Practices הנהוגים בשוק וביצרנים השונים.

2.5.2 באחריות הספק הזוכה להטמיע כל דרישה של המזמין בגין הקשחה של איזו מן המערכות/תשתיות/מוצרים ובלבד שההקשחה אינה מצריכה את הספק ברכש תוכנה/חומרה ייעודיים שלא תוכננו והוצעו על ידו במסגרת המענה למכרז.

2.5.3 על הספק נדרש לעקר רכיבים קורנים לרבות NFC, WIFI ,BT מתחנות הקצה ושרתי המערכת. בנוסף, נדרש לעקר ממשקים שאינם בשימוש כגון: מצלמה, מיקרופון, רמקול וכו'.

2.5.4 על המציע להטמיע הגנה מפני נוזקות ופוגענים באמצעות מוצרי Antivirus/Antimalware שיותקנו על כלל תחנות המשתמשים והשרתים בארגון.

2.5.4.1 זיהוי בין המערכת למדיה יתבסס על אימות Serial Number ברמת מערכת ההפעלה(device control)

2.5.4.2 עדכוני מערכת הפעלה וכלי הגנה יעשו באמצעות התקן חיצוני ייעודי שיאושר ברמת Serial Number ב-device control

2.5.5 הכנסת מידע לרשת המשקף\ תבוצע באמצעות פתרון הלבנה ייעודי שיאופיין שיסופק ע"י המזמין..

2.6 עדכונים וניהול טלאים

2.6.1 על הספק הזוכה לדאוג לכך כי עדכוני מערכות הפעלה ועדכוני אבטחת מידע יתבצעו באופן סדיר ושוטף (אחת לשבועיים). עדכוני אבטחה קריטיים במערכות האבטחה יוטמעו מידית עם הפרסום של העדכון. כמו כן, בכל עדכון גרסה יש לעדכן את מערכת ההפעלה וכלי ההגנה השונים.

2.7 מערך מצלמות אבטחה

2.7.1 יש לוודא מתן גישה למערך המצלמות למשתמשים ,וזאת רק לאחר השלמת בדיקות הנדרשות בהתאם לחוק.

2.7.2 יש לוודא כי מערך המצלמות (מצלמה DVR ,וכדומה) אינו חשוף לאינטרנט. בהינתן כי נדרשת גישה מרחוק יש לנקוט בצעדים הבאים:

2.7.2.1 מתן גישה בהתאם ל Allowlist-פרטני של כתובות מורשות.

2.7.2.2 מתן גישה באמצעות שימוש ב VPN-או SDP.

2.7.2.3 אירוח דף המצלמה כ- Iframe-וחשיפתו כדף אתר אינטרנט המוגן באמצעות WAF ו-IPS.

2.7.2.4 יש לוודא שלא יעשה שימוש ברשת אלחוטית לשם קישור בין רכיבי מצלמות האבטחה.

2.7.2.5 יש לחסום אפשרות לעבודה עם פרוטוקולים פגיעים כגון : FTP,TELNET,TFTP.

2.7.2.6 יש לוודא כי לא נעשה שימוש בסיסמאות ברירת מחדל (Password Default) סיסמאות זהות באתרים/שירותים שונים או סיסמאות קלות לניחוש

2.7.2.7 יש לוודא כי שמירת המידע שנקלט במצלמה ועיבודו עומד בהוראות החוק הרלוונטיות, ובכלל זה חוק הגנת הפרטיות והתקנות מכוחו.

2.7.2.8 יש לוודא כי לא ניתן למחוק או לשנות הקלטות ומידע רלוונטי במשך תקופה מוגדרת. (Retention Data)

2.8 ניטור, איסוף ,ניהול וניתוח לוגים

2.8.1 הספק נדרש לספק מערכות איסוף, ניטור וניתוח לוגים עבור רשתות הפרויקט (רשת המשקף) אשר יחובר לכל מרכיבי הפתרון ללא יוצא מהכלל :

2.8.1.1 מנהלי המערכת, בהתאם להרשאתם, יגדירו מהם הרכיבים אשר הפעילות בהם תתועד בקבצי הלוג ובקבצי החיווי.

2.8.1.2 המערכת תשמור מידע היסטורי על כל פעילות לתקופה פרמטרית שתיקבע ע"י המזמין, לצורך מעקב רוחבי, בדיקות וסקרים של המזמין ומתן מענה משפטי.

2.9 סקרי סיכונים ובדיקות חדירות

2.9.1 למזמין יהיה רשאי לבצע לכלל הרכיבים בפתרון בדיקות חדירות וסקר סיכונים הן לפני חשיפתה והשקתה של המערכת, הן כתנאי להעלאת גרסה ושדרוג התוכנה, והן מדי 18 חודשים מאז הסקר/הבדיקה הקודם/קודמת, וזאת גם אם לא בוצע בה כל שינוי בפרק זמן זה.

2.9.2 כל שינוי מהותי בפתרון הטכנולוגי כפי שימומש ע"י הספק הזוכה, יחייב בביצוע הערכת סיכונים מחודשת ובדיקות חדירות וסקר קוד בהתאם להנחיית תחום אבטחת המידע ברשות המיסים - אגף המכס.

2.9.3 על הספק יהיה - לעדכן את המזמין כי תוקנו כל הליקויים, ככל שיימצאו כאלו, וזאת כתנאי לקבלת אישור להשקת הפתרון או שדרוגו.

2.9.4 הספק הזוכה יאפשר, יסייע, ימסור מידע וילווה את נציגי תחום אבטחת המידע ברשות המיסים - אגף המכס או כל גורם אחר מטעמו בביצוע כל סקר/מבדק/ביקורת שבו המזמין ויעשה כך מיד עם קבלת הדרישה מהמזמין.

גרסא : 1.0	תאריך תחולה:	עמוד 6 מתוך 6
נספח אבטחת מידע והגנה בסייבר להקמת מתחם משקף מעבר ניצנה	תאריך יצירה: 19.03.2023	

2.10 דיווחים ואסקלציה

2.10.1 הספק ימנה, בשיתוף תחום אבטחת המידע ברשות המיסים – אגף המכס, נאמן אבטחת מידע שיהווה איש קשר (Point of Contact) כלפי התחום.

2.10.2 על הספק לדווח מיידית על כל אירוע ו/או חשד לאירוע ו/או אירוע טכנולוגי שמשבית פעילות תקינה של המתקן על כל מערכותיו.

2.10.3 למען הסר ספק, באחריות הספק, לטפל בכל אירוע אבטחת מידע מיד עם זיהויו וגילויו ועד להסרה מלאה של האיום לרבות שימוש בכל המשאבים הדרושים לכך מטעם הספק.
סגירת אירוע סייבר יתאפשר באישור המזמין בלבד בפרט ע"י נציג תחום אבטחת מידע.

2.10.4 הספק מודע שחל איסור מוחלט להוציא רשומות\ואו קבצים ממערכת המשקף. כל הוצאת חומר או רשומה תבוצע באישור תחום אבטחת מידע ברשות המסים- אגף המכס.