משטרת ישראל

- בלמ"ס -

מטא"ר / אגף תמיכה לוגיסטית
מחלקת הרכישות והמכירות
23/05/2024

א.ג.נ.

הנדון: עדכון מס' 3 מכרז 4/2024 כלי בינה עסקית BI

1. תשומת לב המציעים לשינויים:

1.1. **התווסף סעיף 8.7** – הגשת מסמך עמידה בתקן ISO27001 למערכת הרלוונטית.

1.2. **בוצע עדכון בנספח ט'**- דרישות אבט"מ והגנת הסייבר (מצ"ב כנספח)

1.3. **בוצע עדכון בנספח יא'**– נספח הצמדה, עודכן סעיף 2.3 (מצ"ב כנספח)

1.4. **המועד האחרון להגשת הצעות נדחה עד לתאריך 16/06/2024 בשעה 15:00**.

1.5. **לידיעתכם:** מענה לשאלות הבהרה שהתקבלו יפורסם בהמשך.

2. ביתר תנאי המכרז - אין שינוי.

3. יובהר כי:

3.1. כל ההבהרות, השינויים והתיקונים האמורים בעדכון זה, ייחשבו כאילו נכללו במסמכי המכרז מלכתחילה.

3.2. אלא אם נאמר אחרת, לכל המונחים והמושגים האמורים בעדכון זה תהיה הפרשנות כאמור במסמכי המכרז.

3.3. אין להסתמך על כל הסבר או פירוש שניתן בעל פה או בכתב או בכל דרך אחרת על ידי מי מטעם המשטרה או ועדת המכרזים, ככל שניתן, בכל פורום או צורה שהיא. השינויים היחידים מהאמור במסמכי המכרז וכן כל הפירושים וההבהרות להם, הם כמפורט בעדכון זה בלבד ובעדכונים נוספים שיצאו מטעם ועדת המכרזים, ככל שיצאו.

3.4. האמור בעדכון זה אינו משנה או גורע מהאמור במסמכי המכרז אלא אם נאמר במפורש אחרת.

בברכה,

חדוה בשארי, פקד
חו' רכש פרוייקטים טכנולוגים

נספח ט'

דרישות אבט"מ והגנת הסייבר

דרישות אבטחת מידע וסייבר – מכרז פלטפורמת בינה עסקית BI

1. כללי

1.1. מסמך זה מאגד את דרישות אבטחת המידע והגנת הסייבר לצורך התקשרות עם הזוכה ומטרתו להגדיר את רמת אבטחת המידע והגנת הסייבר כתנאי לאספקת השירותים בהתאם לצרכי משטרת ישראל.

1.2. על הזוכה לעמוד בדרישות אבטחת המידע והגנת הסייבר בהתאם לאיומי הסייבר העדכניים.

1.3. במקרה של דרישות אבטחת מידע סותרות, לכאורה, על הספק להציג את הדרישות הסותרות בפני נציג משטרת ישראל, ולענות על הדרישה המחמירה יותר מבין הדרישות הסותרות, אלא אם כן רמ"ד אבטחת מידע והגנת הסייבר הורה לו אחרת, מראש ובכתב.

2. הגדרות ומושגים

2.1. מ"י: משטרת ישראל.

2.2. יחב"מ: יחידת ביטחון במידע במ"י.

2.3. מידע: ידיעה, מסמך, תכתובת, תכנית, נתון, מודל, חוות דעת, מסקנה וכל דבר אחר הקשור ו/או הנוגע למתן השירותים, לרבות מידע הנוגע לצנעת הפרט של עובדי מ"י או האזרח, בכתובים, בע"פ ו/או בכל צורה או דרך של שימור ידיעות בצורה חשמלית ו/או אלקטרונית ו/או אופטית ו/או מגנטית ו/או אחרת, הקשורים ו/או הנוגעים למתן השירותים, אשר אינו מצוי בנחלת הכלל.

2.3.1. <u>שלמות מידע</u> - זהות הנתונים במאגר מידע למקור שממנו נשאבו, בלא ששונו, נמסרו או הושמדו ללא רשות כדין.

2.3.2. <u>סודיות המידע</u> – חשיפת המידע לגורמים לא מורשים.

2.3.3. <u>זמינות המידע</u> – שמירה על נגישות למידע באופן רציף.

2.4. הממונה על אבטחת המידע והגנת הסייבר בצד הזוכה: הזוכה יגדיר איש קשר בעל עולם תוכן טכנולוגי מתאים ורצוי בעל היכרות עם עולם התוכן של איומי הסייבר, אשר יהווה רפרנט אבטחת מידע והגנת הסייבר ליישום ההנחיות המופיעות בנספח זה. פרטיו ודרכי יצירת קשר עמו וזהותו תאושר ע"י משטרת ישראל.

2.5. נכסי המידע: כל המידע, מאגרי המידע, נתון אחר או ציוד של מ"י אשר משמש לצורך פעילות המאגר לצורך הפעלת המכרז.

2.6. מערכות מידע: כלל הציוד הממוכן התומך בעיבוד והצגת המידע של מ"י הכולל בין השאר: שרתים, מחשבים נייחים וניידים, ציוד תקשורת, ציוד אבטחת מידע ועוד.

2.7. אבטחה פיזית: האמצעים הפיזיים הנדרשים להגנה על ציוד המחשוב, לגישה למידע של מ"י ולשרידות המערכות הממוחשבות המכילות את מאגרי המידע.

2.8. התקן נייד: מחשב/אמצעי המיועד לשימוש נייד ובכלל זה טלפון נייד ו/או מצע אחר המשמש לאחסון חומר מחשב.

2.9. סיווג מידע: הקניית הגדרת רגישות למידע, בהתבסס על העקרונות שהוגדרו ע"י מ"י.

2.10. נזק למידע/איום (Threat): פגיעה בסודיות, שלמות וזמינות המידע בבעלות ו/או השייך למ"י.

2.11. אבטחת מידע: הגנה על סודיות, שלמות וזמינות המידע בבעלות ו/או השייך למ"י, הגנה על המידע מפני חשיפה, שימוש או העתקה, והכל ללא רשות כדין.

2.12. אירוע במ"מ/אירוע בטחון מערכות מחשב/אירוע סייבר: פעולה המתבצעת בזדון או בשוגג העלולה לפגוע בזמינות, אמינות וסודיות המידע ו/או בציוד המחשוב של מ"י ברמות שונות, ולהביא להשבתת מערכות, שיבוש נתונים מכוון או חשיפת נתונים לגורמים לא מורשים.

2.13. מנגנון הזדהות: אמצעי המספק פרטים לגבי זהותו של אדם או מערכת בעת ניסיון כניסה ואישור ביצוע פעולות למערכת מידע.

2.14. זיהוי חד ערכי: ערך ייחודי המזהה את מי שמתיימר להיות בעל אמצעי הזיהוי.

2.15. הזדהות חזקה: אמצעי זיהוי המתבסס על לפחות שניים מהפריטים הבאים:

תכונה פיזיולוגית ייחודית של המשתמש – Something You Are

פריט הנמצא ברשות המשתמש – Something You Have
פריט מידע הידוע למשתמש – Something You Know

2.16. הצפנה: יישום של קריפטוגרפיה הממירה מידע גלוי למידע מקודד באופן שיוכל להיות מפוענח ומובן אך ורק לגורמים מורשים.
2.17. Vulnerability - פגיעות: חולשה במערכת העלולה להוביל להתממשות איום.
2.18. מיקור חוץ: השימוש בשירותי מיקור חוץ משמעו הוצאה מחוץ לארגון, או ביצוע על ידי מי שאינם עובדים בארגון.
2.19. זוכה: חברה אשר התמודדה במכרז ונקבעה כזוכה ע"י וועדת המכרזים של משטרת ישראל.

3. השיטה, חוקים ותקנים

3.1. הזוכה ימנה נאמן אבטחת מידע והגנת הסייבר, אשר יהווה רפרנט אבטחת מידע והגנת הסייבר ויהיה אחראי ליישום כלל היבטי אבטחת המידע במערכות ובתהליכים.
3.2. הזוכה מתחייב לעמוד בהוראות חוק המחשבים, תשנ"ה-1995.
3.3. הזוכה מתחייב לעמוד בדיני הגנת הפרטיות ובכללם חוק הגנת הפרטיות, תשמ"א-1981 ותקנות הגנת הפרטיות (אבטחת מידע) תשע"ז-2017.
3.4. הזוכה מתחייב ליישם את הנחיות מערך הסייבר הלאומי, באופן שהולם את פעילותו, גודלו ומורכבותו, ותוך ניהול הסיכון כפונקציה של הסתברות והשפעה. תכניות העבודה ליישום הבקרות על-פי תורת ההגנה תיקבע בהתאם להנחיות הרגולטור (במידה וקיים) ו/או בהתאם לתכנית בקרות שתתואם בין שני הצדדים.
3.5. הזוכה מתחייב לעמוד בהנחיות הגוף האסדרתי (רגולטור) אליו הוא כפוף (במידה וקיים).
3.6. בהתאם להחלטת ממשלה 2443, הספק מתחייב לעמוד בתקן ISO27001 למערכת הרלוונטית, המציע נדרש להגיש את המסמך הרלוונטי בעת הגשת ההצעה כמפורט בסעיף 8.7 במכרז.
3.7. הזוכה מתחייב כי בכל מקרה בו הוא מחזיק ברשומות אשר מכילות מידע פרטי של המזמין, כהגדרתם בתקן PCI-DSS של חברות האשראי הבין לאומיות, הזוכה יעמוד בכל הוראות התקן הרלוונטיות לעניין זה.
3.8. יש לפרט תקנים נוספים בהם השירות עומד כגון: CSA STAR level 2 , ISO27018, SOC2, GDPR וכד' ככל וקיימים.
3.9. רכש מוצר ו/או רכיב במוצר ו/או קו הייצור לא יהיו מבית יצרן המצוי ברשימה שנאסרה על ידי ה-NDAA.
3.10. ככל שמיושם פתרון לשמירת מפתחות הצפנה, על המערכת/הספק לעמוד בתקן FIPS 140-2 level 2 ומעלה עבור המודולים הקריפטוגרפים של המערכת.
3.11. הנתונים הפרטיים של משתמשי מ"י או מי מטעמה יהיו חסויים וללא סממני תיוג שיוך ארגוניים, הן בשלב המכרז והן לאחריו ללא הגבלת זמן.
3.12. אי יישום העקרונות המובאים במסמך זה בחלקם או במלואם עלול להביא לפסילת ההתקשרות מול הזוכה או להפסקתה בהתאם לשיקול דעתה של מ"י.

4. תפישת האבטחה

4.1. תפישת האבטחה:
4.1.1. שירותי/מערכת הזוכה יעמדו בהתאם להנחיות משטרת ישראל, לרבות מדיניות אבטחת מידע, מדיניות פיתוח מערכות מאובטחות, תקן צומת השירותים המבוסס על תקן Web Services Security האמריקאי, מדיניות מערכות מנהלות משתמשים, מדיניות סיסמאות, מדיניות אירוח של משטרת ישראל והכללים לביצוע בדיקות חוסן.
4.1.2. שירותי/מערכת הזוכה יעמדו בעקרונות הגנת הסייבר ואבטחת המידע במטרה להבטיח את הרציפות התפקודית בהיבטים הבאים:
א. אמינות המערכות והמידע
ב. זמינות המערכת והמידע
ג. סודיות המידע, לרבות נתוני המערכת

4.1.3. שירותי/מערכת הזוכה יישמו את העקרונות הבאים מול ממשקי הניהול ושאר ממשקי המערכת:

א. Identification – אמצעי הזיהוי
ב. Verification – אימות הזיהוי
ג. Authentication – תצורת רכיב הזהות וההזדהות בתהליך הכניסה לשירות ובמהלך הפעילות האפליקטיבית
ד. Authorization – תהליך אשרור אלמנט הזהות וההזדהות בתהליך הכניסה לשירות ובמהלך הפעילות האפליקטיבית
ה. Access control – בקרת גישה בהתאם לכל רכיב במערכת
ו. Reliability – מהימנות המידע
ז. Confidentiality – סודיות המידע, הגנה על מידע רגיש (הצפנה)
ח. Data integrity – שלמות המידע
ט. Non-repudiation – מניעת התכחשות
י. Log, Audit, Monitor – תיעוד, רישום, ניטור

4.2. הזוכה מתחייב להשתמש במערכות הפעלה עדכניות המעודכנות בטלאי האבטחה העדכניים ביותר. הזוכה יישם מדיניות התקנת טלאים עיתית.

4.3. הזוכה יממש סגמנטציה והפרדה מיטבית בין הרכיבים השונים (WEBSERVER, DB וכד') של חלקי המערכת המספקים שירות למשטרת ישראל, מסמך מדיניות סגמנטציה לדוגמה יועבר בנפרד לזוכה על ידי משטרת ישראל לאחר זכייתו, ככל שיבקש.

4.4. הספק ידווח אודות כל חולשה או פגיעות שתמצא באחד רכיבי החומרה ו/או התוכנה המסופקים למ"י במסגרת ההתקשרות באופן מידי.

5. שרשרת האספקה

5.1. מ"י מנהלת את סיכוני הסייבר אליה היא חשופה מצד נותני השירות שלה. במסגרת ניהול הסיכונים ועמידה ברגולציה, מ"י בודקת את רמת התאמתם של הספקים השונים המהווים חוליה בשרשרת האספקה שלה. כחלק מבדיקת התאמתו של הזוכה יבחנו סיכוני סייבר פוטנציאליים הנובעים מההתקשרות וזאת בין היתר על ידי הגדרת תהליכי עבודה מאובטחים ויישום והטמעת בקרות להפחתת החשיפה לסיכוני סייבר. בדיקה זאת יכולה להתבצע טרם ההתקשרות ובמהלך ההתקשרות של מ"י עם הספק.

5.2. הבדיקה מתבצעת באמצעות מילוי שאלון במערכת מידע הנשלח ע"י מ"י ובדיקה נוספת באמצעים גלויים על הספק. העדר מילוי השאלון ואי עמידה בתנאי הניקוד של הבדיקה שנקבעו למכרז ע"י מדור אבטחת מידע והגנת הסייבר במ"י יכולה להוות עילה לסיום ההתקשרות עם הזוכה.

5.3. אחת לשנה באחריות הזוכה למלא מחדש את השאלון.

5.4. בדיקת ובחינת חוסן הסייבר של ספקי מ"י מתבצעת באופן שוטף, הזוכה מתחייב לתקן כל פגיעות שתתגלה במהלך ההתקשרות אשר תפגע בחוסן הסייבר שלו, באופן מיידי לאחר קבלת בקשה מטעם משטרת ישראל.

6. סיווג מידע ושמירה על סודיות ופרטיות

6.1. באחריות הזוכה לדאוג לחיסיון, אמינות וזמינות המידע של מ"י שברשותו.

6.2. הזוכה יהיה אחראי לכל עקיפה או ניסיון עקיפת מנגנוני אבטחה ובקרות גישה לתשתיות שונות, שיבוצע על ידי מי מהעובדים ו/או נותני השירותים מטעמו.

6.3. בכל מקרה של אירוע ביטחון מידע / אבטחת מידע / סייבר או אירוע חריג או שקיים חשד לאירוע כזה, הקשור לשירותים ו/או נכסים של מ"י או שיש עמו השלכה ישירה או עקיפה על ביטחון מערכות המידע ו/או המידע של מ"י, הזוכה נדרש להודיע באופן מידי לאיש הקשר מטעם מ"י, לשתף פעולה, מידע וממצאים עם מ"י ומ"י תהא רשאית להצטרף לניהול האירוע ע"י הזוכה בתיאום מולו.

6.4. על הזוכה ליישם יכולת הגדרה במערכי הניטור לרישום גישה או ניסיונות גישה למידע המוגדר כרגיש או מסווג.

6.5. בעת פיתוח/הקמת מערכת ייעודית עבור מ"י, הזוכה מתחייב להפריד ככל הניתן, הפרדה מלאה את מאגרי מ"י המצויים בידיו ברמה פיזית מיתר מאגרי המידע שברשותו. במידה ולא מתאפשר יש לקבל אישור בכתב ומראש לכך ממדור אבט"מ והגנת הסייבר במ"י. מ"י רשאית לבצע בקרה תהליכית וטכנולוגית אצל הזוכה, לאחר תיאום עמו. הזוכה מתחייב לשתף פעולה עם נציגי מ"י לצורך כך.

6.7. הזוכה מתחייב שלא להשתמש בעבור שירותיו למ"י, בשירותי ענן (Cloud) מכל סוג שהוא או שירותי מחשוב חיצוניים מבלי שאלה אושרו מול מ"י.

7. אבטחת המידע במישור משאבי האנוש והעובדים

7.1. על הזוכה לבצע הדרכות למודעות אבטחת מידע והגנת הסייבר לעובדיו בתחום העיסוק של העובד בתדירות של אחת לשנה. בנוסף, יבצע לעובדיו העוסקים בפעילות מול ו/או עבור מ"י, הדרכת ריענון ועדכון בנושא מדיניות, הנחיות, ונוהלי הגנת מידע כפי שמתחייבים מהסכם ו/או התקשרות זו. באחריות הספק לבצע מעקב ותיעוד אחר ההדרכות הנ"ל ולהציגן על פי דרישה לנציג מ"י.

7.2. הספק מתחייב למנוע מקרים בהם עובדיו ו/או מי מטעמו ינסו לבצע גישות למאגרים אליהם לא קיבלו הרשאה. במידה ואיתר הזוכה גישה בלתי מורשית לנתוני מ"י, באחריותו לדווח למדור אבטחת מידע והגנת הסייבר במ"י אודות האירוע.

7.3. הזוכה מתחייב כי תפקידים ותחומי אחריות של עובדי הזוכה ו/או מי מטעמו ו/או משתמשי צד שלישי הנוגעים לאבטחה, יוגדרו ויתועדו ע"י הזוכה.

8. סיום התקשרות

8.1. בסיום ההתקשרות הזוכה יחתום על הצהרה בה הוא מתחייב שלא נשארו ברשותו מידע או מערכות מידע או ציוד הנוגע למ"י. נדרש לוודא עמידה בכל הקשור למחיקת והחזרת מערכות מידע ומידע של מ"י המאוחסנים בחצרי הזוכה ומי מטעמו בתום ההתקשרות בין הצדדים, כולל רשומות, מדיה, ציוד ורכיבים.

8.2. באחריות הזוכה לוודא כי לא נותרות הרשאות גישה, אמצעי הזדהות וגישה פיזית ו/או לוגית למידע של מ"י.

9. אפיון השירות המוצע

9.1. הזוכה מתחייב להגיש מסמך המתאר את מדיניות אבטחת המידע והגנת הסייבר של השירות המוצע, יש להתייחס למערכת המוצעת ולמערכות המידע בהם תפותח המערכת ו/או יוחזק מידע של משטרת ישראל.

9.2. הפירוט יכלול:

9.2.1. תיאור ארכיטקטורה של המערכת/השירות המוצע.

9.2.2. בקרות אבטחת המידע והגנת הסייבר אשר בשימוש המערכת/השירות.

9.2.3. ההפרדה הקיימת ברמת חומרה ותוכנה ותקשורת בין מערכות הזוכה לבין מערכת הזוכה המיועדת עבור מ"י, בכל אחד מרכיבי המערכת אצל הזוכה.

9.2.4. התייחסות לסביבות PROD ו- TEST עבור מ"י.

9.2.5. הגנה פיסית וסביבתית.

9.2.6. המשכיות עסקית, נהלי גיבוי ו-DR.

9.2.7. אופן שילוב תהליך SDLC במחזור חיי המערכת/השירות.

9.2.8. תהליכים ארגוניים לצמצום סיכונים והתמודדות עם איומים.

9.2.9. המצאות והערכה של תאימות לתקינה ולחוקים.

9.2.10. אופן זיהוי ותגובה לאירועים.

9.2.11. הערכת עובדים ובדיקות מהימנות.

9.2.12. ביצוע מבדקי חדירה תקופתיים.

9.2.13. יישום מנגנוני ניטור ובקרה.

9.2.14. אופן הטיפול בנושא הזדהות וניהול הרשאות.

9.2.15. זיהוי חולשות והתקנת טלאים.

9.2.16. במידה והמציע 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.

10. אבטחה פיזית וסביבתית בחצר הספק

10.1. הזוכה 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.

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

10.3. אמצעים לבקרת כניסה פיסית: הזוכה 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.

10.4. הזוכה מתחייב לכתוב וליישם הנחיות אבטחה פיזית לעבודה באזורים הייעודיים.

10.5. כל מידע/מדיית זיכרון שהכילה מידע רגיש ו/או מסווג תוצא אל מחוץ לזוכה לצורכי תחזוקה רק לאחר שננקטו אמצעים מספקים למחיקת המידע באופן המונע אפשרות שחזור המידע באמצעים טכנולוגים גם לאחר מחיקת המידע ובאישור מדור אבט"מ והגנת סייבר במ"י.

11. אבטחה לוגית ברשת המחשוב של הספק

11.1. הספק מתחייב ליישם את דרישות "תורת ההגנה בסייבר לארגון" של מערך הסייבר הלאומי, באופן שהולם את פעילותו, גודלו ומורכבותו, ותוך ניהול הסיכון כפונקציה של הסתברות והשפעה.

11.2. המציע מתחייב ליישם אמצעי אבטחת מידע והגנת הסייבר הולמים שימנעו חדירה מכוונת או מקרית למערכת או למערכות התשתית והתקשורת, יש לפרט במענה לסעיף 9.1 את אמצעי הבקרה שהספק מציע.

11.3. הזוכה מתחייב כי מערכות ומאגרי המידע של מ"י (במידה ויש) לא יחוברו לסביבת האינטרנט, אלא אם כן קיבל את אישור מ"י לכך.

11.4. במידה וקיבל הזוכה אישור וחיבר את המערכות ו/או מאגרי המידע לרשת ציבורית או לאינטרנט, מתחייב הזוכה לנקוט באמצעי ההגנה המתאימים על מנת למנוע נזק, פריצה, זיהום או השחתה של מאגרי המידע, יש לפרט את הצעת הספק להתמודד עם האיומים הנ"ל ולצרף למענה את רשימת הבקרות והאמצעים הנותנים מענה לדרישה.

11.5. הזוכה מתחייב שהעברת המידע בתוך רשת התקשורת, ברשת ציבורית או על גבי רשת האינטרנט תיעשה תוך שימוש בשיטות הצפנה מקובלות, בפרוטוקולים סטנדרטיים, המקובלים והחזקים ביותר בלבד.

11.6. על ציוד הקצה המשמש להעברת תקשורת (מתגים, נתבים, FW) לעבור הקשחות בהתאם למדיניות היצרן ולעבור עדכוני קושחה עיתיים.

11.7. הקשחת הרכיבים תתבסס על שני עקרונות:

11.7.1. נטרול שירותים, הרשאות ותפקידים לא נחוצים.

11.7.2. מזעור אפשרויות גישה ותיעוד (לוגים) מקסימאלי.

11.8. הזוכה מתחייב לבצע הפרדה בין רשתות המאכלסות את המידע/מאגרי המידע של מ"י (במידה ויש) ליישומים ולכלל הרשתות (סגמנטציה) באמצעות הפרדה לוגית הכוללת סגמנט מבודד מאחורי חומת אש.

11.9. חל איסור מוחלט לשמור מידע רגיש בתחנה מרוחקת של המשתמש שלא הותאמה למדיניות מסמך זה.

11.10. מחשבי הזוכה מהם ניתן לגשת למידע של מ"י ולמערכותיו, יצוידו במערכת הפעלה ובתוכנות אנטי וירוס מעודכנות ונתמכות לצורך הגנה מפני קוד זדוני (וירוסים, תולעים, סוסים טרויאנים ותוכנות רוגלה אחרות).

11.11. הזוכה מתחייב להתקין רכיב סינון תוכן (Content Filtering) אשר ימנע כניסה של קוד לרשת הזוכה בעת גלישה לאינטרנט ושימוש בדוא"ל.

11.12. הזוכה מתחייב לעשות ככל הניתן על מנת שכל מערכות ההפעלה ואמצעי אבטחת המידע והגנת הסייבר יוקשחו לפי המלצות היצרן,Best Practices ודרישות מ"י.

11.13. הזוכה מתחייב לעדכן באופן שוטף את המערכות השונות למניעת ניצול פרצות אבטחת מידע.
11.14. הזוכה מתחייב שמערכות אבטחת מידע יספקו שרידות מלאה לשמירה על זמינות המערכת.
11.15. הזוכה מתחייב להתקין אמצעי מפני חדירה לא מורשית למערכת והכנסת רכיבים לא מורשים.
11.16. הזוכה מתחייב להתקין אמצעי הגנה למניעת זליגת מידע (DLP) מהמערכת ובקרה אחר המידע היוצא מהמערכת ומרשת המחשוב.
11.17. במאגר מידע שניתן להתחבר אליו מרחוק למטרות ניהול, הזוכה מתחייב לבצע הזדהות חזקה (MFA) ובקרות הגנה מתאימות.

12. תקשורת וממשק מול רשתות מחשוב של מ"י

12.1. לזוכה לא תאופשר גישה מרחוק לרשתות/מערכות/תחנות/רכיבים אם יותקנו במתקני משטרת ישראל. במקרה של תקלה הזוכה יצטרך להגיע פיזית לאתר משטרת ישראל.
12.2. במידה ונדרשת העברת קבצים בין הארגונים, העברה תתבסס על פתרון א-סינכרוני דוגמת Waterfall וטכנולוגיית כספת (MFT) כדוגמת GoAnyWhere.
12.3. משטרת ישראל שומרת לעצמה את הזכות לעבור לטכנולוגיה אחרת (במקום GoAnyWhere), ובמצב זה על הזוכה להתאים את המערכות לעבודה עם מ"י על חשבונו.

13. גיבוי, שחזור והתאוששות

13.1. מידע של מ"י (במידה ויש), הנמצא במערכות הזוכה יגובה בצורה סדירה על פי מדיניות הזוכה.
13.2. הזוכה מתחייב לבצע גיבויים מאובטחים של המידע הנצבר אצלו תוך הבטחת שלמותם ואמינות, לשם אפשרות שחזור המידע ושמירת הרציפות העסקית.
13.3. במידה ויש שימוש בספקי צד שלישי לאחסון גיבויים, יש לעדכן את גורמי מ"י ולוודא עמידתם בכל הדרישות המוגדרות במכרז זה.
13.4. הזוכה מתחייב לבצע שחזורים מדגמיים של המדיות המגובות על תשתיותיו לצורך בדיקת התאוששות.
13.5. הזוכה מתחייב כי במידה ובוצע שחזור יתועדו כל הליכי השחזור כולל זהותו של מבצע השחזור.
13.6. הזוכה מתחייב למנוע עירוב מידע מסיווגים שונים בזמן השחזור.

14. פיקוח וביקורות תקופתיות

14.1. הזוכה מתחייב לבצע מדי שנה וחצי סקר אבטחת מידע (Security Audit) ו/או מבדק חדירה (Penetration Test) לרשת התקשורת שלו ולמערכות שלו על ידי גורם צד שלישי בעל הכשרה והסמכות מתאימות, וכן להעביר או להציג את ממצאי הסקר ומבדק החדירה לעיונו של מדור אבטחת מידע והגנת הסייבר במ"י. על הזוכה להציג נוהל טיפול בממצאים וליקויים שעלו במבדקים וסקרים אלו לרבות SLA.
14.2. מ"י רשאית לערוך ביקורות (באמצעות מדור אבטחת מידע והגנת הסייבר של מ"י ו/או ע"י ספק חיצוני המועסק מטעמו) בחצרי או במערכות הספק (מעבר לאלה שתערוך חברת אבטחת המידע בה יבחר הזוכה) לשם ווידוא עמידה בהנחיות מסמך זה ו/או לצורך זיהוי כל סיכון אפשרי על המידע של מ"י. ביקורות אלו יעשו בתיאום אל מול הזוכה ועשויות לכלול, על פי שיקול דעתה של מ"י, את אלה:
    14.2.1. בקרה על תהליכי ונהלי עבודה רלוונטיים לעבודת הזוכה מול מ"י;
    14.2.2. יישום אמצעי אבטחת המשאב האנושי בחצרות הזוכה;
    14.2.3. יישום אמצעי אבטחה פיסית וסביבתית בחצרות הזוכה;
    14.2.4. יישום אמצעי אבטחה לוגית בחצרות הזוכה (כולל כניסה למערכות הזוכה ו/או בדיקה באמצעות כלים ממוכנים ברשת ומערכות הזוכה);
    14.2.5. בחינת חוסן מערכות המידע של הזוכה מתוך או מחוץ לרשת הזוכה על ידי גורם חיצוני בלתי תלוי, כפי שיוגדר על ידי מ"י (תוך תיאום עם הזוכה ובהסכמתו).

14.2.6. טיפול בממצאי הבדיקות – הזוכה מתחייב לטפל בכל הממצאים ובהתאם להנחיות שיועברו לו על ידי משטרת ישראל ולתקן כל הנדרש.

15. פיתוח תוכנה

15.1. בכל הנוגע לפיתוח תוכנה על הזוכה לעמוד בסטנדרטים ותקינה המקובלים בעולם בנושא פיתוח מאובטח כמו OWASP, ISO, NIST וכד'.

15.2. הזוכה נדרש לשלב את תהליכי ההגנה בסייבר כחלק אינטגרלי בניהול מחזור פיתוח תוכנה SDLC – Software Development Life Cycle .

15.3. קוד התוכנה יכיל רק את הנרשם בתיעוד המסופק עם התוכנה ואשר סוכם בעוד מועד עם משטרת ישראל.

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

15.5. התוכנה תיבדק ע"י בודקי חדירות בלתי תלויים, בתהליך Code Review בצורה מעמיקה, כולל תיקון באגים הפוגעים באבטחת המידע והגנת הסייבר של המערכת. פגיעות זו, במידה וקיימת תתוקן ודיווח יועבר למ"י.

15.6. הקוד ייסרק באמצעי SAST (Static Application Security Testing) ו- DAST (Dynamic Application Security Testing) וליקויי האבטחה אשר יופיעו בדו"ח הסריקה יתוקנו בטרם מסירתם למ"י.

15.7. המערכת לא תבצע שינויי קוד במערכות נלוות כגון מערכת ההפעלה אשר פוגעים ברמת האבטחה הכללית של מערכות המחשוב.

15.8. הזוכה מתחייב כי בגרסאות עתידיות של המערכת במידה ויהיו, לא יתבצעו שינויים מהותיים אשר יפגעו ברמת אבטחת המידע והגנת הסייבר במערכת ללא אישור מראש ממדור אבטחת המידע והגנת בסייבר במ"י.

15.9. כל מערכת/תוכנה שתועבר למ"י במסגרת ההתקשרות תיבדק, תזוכה ותאושר ע"י מדור אבטחת המידע והגנת הסייבר במ"י. הזוכה מתחייב לתקן כל ליקוי/פגיעות אשר תמצא בתיאום מול מדור זה ולשביעות רצונו.

דרישות מערכת

16. ניטור, תיעוד ובקרה

16.1. על המערכת לכלול תמיכה בהעברת קבצי לוג ואירועים למערכות אוטומציה וניטור אבטחתי כגון SIEM ו- SOAR כגון SYSLOG.

16.2. על המערכת לכלול רישום ותיעוד מסודר ורציף ללוג (Log) של כל גישה, שינוי הגדרות ופעילות משתמשים וקבצים במערכת וע"פ הפירוט הבא:

16.2.1. שימוש במנגנון ההזדהות - Login\Logout

16.2.2. ניסיון כושל בכניסה למערכת.

16.2.3. ניסיונות גישה למידע ללא הרשאת גישה.

16.2.4. אירועים אפליקטיביים שיוגדרו כדורשי בקרה עפ"י מנגנון כללים מיוחד לנושא.

16.2.5. מחיקת אובייקטים במערכת.

16.2.6. פעילויות המבוצעות על-ידי גורמים בעלי הרשאות גבוהות.

16.2.7. פעולות אדמיניסטרציה (ניהול משתמשים, הורדה והעלאת Services וכד').

16.2.8. שגיאות תפעוליות (נפילת מערכת, הודעות שגיאות תוכנה וכד').

16.3. עבור כל אירוע המוגדר כדורש בקרה יישמרו הפרטים הבאים למשך חצי שנה לפחות:

16.3.1. תאריך ושעה.

16.3.2. מקור ביצוע הפעולה לדוגמה: כתובת IP\DOMAIN.

16.3.3. שם המשתמש.

16.3.4. סוג האירוע.

16.3.5. הצלחה או כישלון של האירוע.

16.3.6. זיהוי האובייקט עליו מבוצעת הפעולה לדוגמא: שם קובץ.
16.3.7. תיאור הפעולה (מה בוצע): עבור כל סוג אירוע יש לספק תוכן רלוונטי. למשל: עדכון רשומה, ניסיון גישה לרשומה, מחיקת משתמש, הורדת מערכת וכד'.
16.4. ההודעות צריכות להיות אמינות, מלאות וברורות.

17. ניהול משתמשים והרשאות במערכת

17.1. המערכת תתמוך במנגנון הזדהות אחודה (SSO - Single Sign On) ובפרוטוקולי הזדהות סטנדרטיים כגון SAML, OpenID, OAuth .
17.2. המערכת תתמוך במנגנון אימות רב-גורמי (MFA - Multi Factor Authentication), נדרש פירוט לגבי כלל מנגנוני ופרוטוקולי ההזדהות הנתמכים במערכת (יש לפרט את פרוטוקולי ההזדהות הנתמכים (כגון U2F, FIDO, OTP)- יש לפרט את יכולת ההתממשקות עם כלי IAM למערכות ניהול משתמשים ולמערכות צד ג' לניהול זהויות
17.3. המערכת תתמוך ביכולת החלת מדיניות סיסמאות למשתמשי המערכת (לרבות משתמשים מקומיים), אשר תכלול קביעה של משתנים כגון: אורך, מורכבות, תוקף, היסטוריית סיסמאות, אכיפת MFA וכדומה.
17.4. המערכת נדרשת לאפשר הרשאות גישה מצומצמות ככל האפשר (Least Privilege) לביצוע פעולות מורשות למשתמשי המערכת, ובכדי להגן על הנתונים מפני גישה לא מורשית, חשיפה, שיבוש, שינוי או מחיקה. נדרש פירוט לגבי אופן ביצוע הגבלת הרשאות הגישה בפתרון המוצע.
17.5. על המערכת לכלול מנגנוני ניהול הרשאות ובקרת גישה מבוססת תפקידים ותכונות
RBAC – Role Based Access Control
ABAC – Attribute Based Access Control
17.6. יידרש פירוט לגבי:
1. סוגי התפקידים (Roles) הקיימים במערכת לבקרת גישה.
2. סוגי החוקים (Rules) הקיימים במערכת לבקרת גישה.
3. פרמטרים אשר לפיהם ניתן לקבוע מדיניות הרשאות גישה לפעולות השונות ולהגביל דינמית גישת משתמשים למערכת כדוגמת סוג משתמש, תאריך, יום, שעת גישה, כתובת IP, נכס מטרה, מיקום גאוגרפי וכד'
4. מזעור אפשרויות גישה ותיעוד (לוגים) מקסימאלי.

18. הצפנת המידע במערכת

18.1. על המערכת לתמוך בהצפנת המידע והתקשורת מקצה לקצה, הן המידע שבתנועה והן המידע שבמנוחה, למול כלל רכיבי המערכת הפנימיים והמנוהלים לרבות בסיסי נתונים, עמדות קצה, שרתים וכדומה.
18.2. על המערכת לתמוך בפרוטוקולי הצפנה סטנדרטיים, המקובלים והחזקים ביותר בלבד, דוגמת AES 256bit גודל מפתח 2048 ומעלה.
18.3. על המערכת/הספק לתמוך בשמירת מפתחות ההצפנה במערכות אבטחת חומרה(HSM) ושירותי ניהול מפתח (KMS) ו/או בכל פתרון אחר המספק הגנה על המפתחות כמתואר בסעיף זה. על הספק להציג כיצד מיישם מענה זה.
18.4. ככל שמיושם פתרון לשמירת מפתחות הצפנה, על המערכת/הזוכה לתמוך בתקן FIPS 140-2 level 2 ומעלה עבור המודולים הקריפטוגרפים של המערכת. נדרש פירוט לגבי אופן הפתרון.

צרופה א' - נספח שמירת סודיות משטרת ישראל

1.1. מובהר בזאת כי ידוע לי (שם מלא ותעודת זהות) _____ אשר לאור אופיו הביטחוני והמבצעי של משטרת ישראל ולאור האחריות בה היא נושאת בנוגע למידע רגיש, הרי שנושא הגנת המידע הינו בעל חשיבות עליונה עבור משטרת ישראל וכי הפרה של כללי הגנת המידע עלולים להסב למשטרת ישראל ומדינת ישראל נזקים בלתי הפיכים ובלתי מדידים. לאור האמור, הרי שהפרה של איזו מן ההוראות המפורטות בכתב התחייבות זה תחשב להפרה יסודית של תנאי המכרז ו/או ההסכם (במידה וקיים) על ידי ה זוכה ומשטרת ישראל תהא רשאית לבטל את ההתקשרות באופן מידי ולזוכה לא תהיה כל טענה ו/או דרישה בשל כך.

1.2. הנני מתחייב לשמור בסודיות מוחלטת כל מידע, לרבות תכנית, חומר בין בכתב ובין בעל פה, מסמך עיוני או מידע מעשי, שהגיע או שיגיע אליי תוך כדי ועקב ביצוע עבודתה עבור משטרת ישראל, ולא לגלותו ו/או להעבירו לאחר, אלא ככל שיידרש ובמידה שתידרש במסגרת ביצוע עבודתי עבור משטרת ישראל ולאחר אישור מראש ובכתב של הממונה על אבטחת מידע והגנת הסייבר במשטרת ישראל. לעניין מסמך זה "מידע" פירושו כל המפורט לעיל, אשר מעצם טבעו או על פי הדין הוא חסוי, לרבות אך מבלי לגרוע מכלליות האמור:

1.2.1. כל מידע הנוגע לפרטים האישיים של עובדי משטרת ישראל, הרלוונטי לנשוא מכרז זה.

1.2.2. כל מידע ניהולי, מידע עסקי ומידע פיננסי, ובכלל זה כל מידע הנוגע לעניינים הכספיים, שיטות העבודה, טכנולוגיות, תהליכי המחשוב, התקשרויות, הספקים והלקוחות של משטרת ישראל.

1.2.3. כל מידע של משטרת ישראל, אשר יגיע לידיעתה ואשר אינו נחלת הכלל.

1.2.4. כל מידע המוגדר כ"מידע רגיש" כהגדרתו בחוק הגנת הפרטיות התשמ"א, 1981.

1.3. הנני מצהיר אשר ידוע לי כי המידע לרבות המידע אשר יעובד במערכות של משטרת ישראל או מידע עבור משטרת ישראל אשר אייצר במסגרת התקשרות זו, הוא בבעלותה הבלעדית של משטרת ישראל, וכי אני לא אהיה רשאי לעשות בו כל שימוש שאינו לצורך ביצוע ההתקשרות עם משטרת ישראל על פי הסכם זה בזמן ההתקשרות ולאחריה ללא הגבלת זמן.

1.4. הנני מצהיר שידוע לי שכל מידע שיתקבל אצלי במהלך מתן השירותים הוא בגדר סודות מקצועיים ומתחייב שלא להעביר מידע ו/או כל חלק ממנו אשר הועבר אליי או נוצר אצלי עבור משטרת ישראל במסגרת הסכם זה לצד ג' בלא קבלת הסכמה מראש ובכתב מאת הגורם שהוסמך לכך מטעם משטרת ישראל לצורך הסכם ו/או התקשרות זו ו/או מכוחם או מערך ביטחון המידע של משטרת ישראל.

1.5. אני אדאג לאבטחת כל מידע שיגיע אליי במסגרת ביצוע התחייבויותיו על פי הסכם זה ואהיה אחראי כלפי משטרת ישראל על כל המידע המועבר אליי או דרכי לרבות דוחות, נתונים אישיים, תכתובות דוא"ל, קבצים ,מסמכים ,שרטוטים וכיו"ב על פי ההנחיות שיועברו על ידי משטרת ישראל.

1.6. באחריותי לדאוג לחיסיון, אמינות וזמינות המידע של משטרת ישראל שברשותי.

1.7. בעת אירוע אבטחת מידע או אירוע חריג, בו קיים חשד לגבי דלף ו/או פגיעה במידע של משטרת ישראל, הנני מתחייב להודיע באופן מידי לאיש הקשר מטעם משטרת ישראל.

1.8. הנני מתחייב לשתף פעולה עם משטרת ישראל בכל אירוע חריג בו מעורב, או שקיים חשד למעורבות שיש עמה השלכה ישירה או עקיפה על ביטחון מערכות המידע ו/או המידע של משטרת ישראל. בכל הפרה או חשד להפרה של חוקים תקנות או נהלי אבטחת מידע כולל בחקירת אירועים או חשדות לחריגות אבטחת מידע או דליפת מידע של משטרת ישראל לגורמים בלתי מורשים.

1.9. מידע רגיש או מסווג יהיה נגיש לעובדי הזוכה ע"פ הגדרת הצורך לדעת (Need to Know) ולעובדים אשר אושרו ע"י משטרת ישראל בלבד.

1.10. הכנת עותקים לצרכי עבודה אצל הזוכה תיעשה על פי צורך בלבד ותפוצתם תהא בקרב עובדי הספק הנדרשים לעותקים אלו בלבד.

1.11. הנני מתחייב לעבוד ע"פ מדיניות "שולחן נקי" - מצב בו מבוצעת פעולה שתמנע גישת זרים למידע רגיש ו/או חסוי אישי, בעת שאת/ה עוזב /ת את סביבת עבודתך , באופן הבא:

1.11.1. ביצוע פעולת Lock (נעילה) במחשב עליו עבדת .

1.11.2. נעילת כל המסמכים בהם מידע רגיש ו/או חסוי אישי.

1.11.3. זיהוי ודאי - תהליך בו זוהה אדם באמצעות תעודה מזהה עם תמונה (ת"ז, דרכון, רישיון נהיגה) או אימות של – פרט סודי שידוע ללקוח ומאומת מול מערכות המידע של משטרת ישראל.

ולראייה באתי על החתום:

תאריך_____ שם_____

ת"ז_____ חתימה_____

נספח יא'

נספח הצמדה

1. הגדרות בנושא הצמדה

1.1. הצמדה - הסדר הנערך במסגרת התקשרות, אשר נועד להתאים את ערך הנכס, השירות או המחיר, לשינויים ברמת המחירים, בהסתמך על פרסומי הלשכה המרכזית לסטטיסטיקה, בנק ישראל או פרסומים רשמיים ובלתי תלויים אחרים, מישראל ומחוץ לישראל. ההצמדה מחושבת ע"י השוואת ערך המדד בתאריך הקובע ביחס לתאריך הבסיס.

1.2. תאריך קובע - המועד על פיו נקבע המדד הקובע, לצורך תשלום ההצמדה עבור תקופה מוגדרת.

1.3. תאריך בסיס - המועד שממנו ואילך מחושבת ההצמדה, לאורך כל תקופת ההתקשרות.

1.4. מדד קובע - ערך המדד בתאריך הקובע, בהתאם לסוג ההצמדה (הצמדה למדד ידוע).

1.5. מדד בסיס - ערך המדד בתאריך הבסיס, בהתאם להצמדה למדד ידוע (הצמדה למדד ידוע).

1.6. מדד ידוע - המדד האחרון שפורסם באופן רשמי, נכון לתאריך הקובע.

2. תנאי ההצמדה

2.1. תאריך הבסיס - המועד האחרון להגשת הצעת המחיר הסופית.

2.2. התאריך הקובע - תאריך החשבונית.

2.3. סוג ההצמדה – שער הדולר ארה"ב.

2.4. סוג המדד - מדד ידוע.

2.5. תדירות ההצמדה - חודשית (ביחס לסוגי מדדים שונים) / יומית (בשער חליפין).

2.6. חלקיות ההצמדה - 100%.

3. ביצוע ההצמדה

3.1. ביצוע ההצמדה יחל מהחשבונית הראשונה להתקשרות.

3.2. ביצוע ההצמדה יהיה גם במקרים בהם מדובר בהצמדה שלילית.

3.3. אופן חישוב ההצמדה

3.3.1. חישוב ההצמדה יתייחס לשינוי בסוג ההצמדה בין תאריך הבסיס לבין התאריך הקובע וזאת בהתאם לתנאי ההצמדה המפורטים בסעיף 2 לעיל.

3.3.2. חישוב ההצמדה יפורט ע"ג החשבונית.

3.3.3. ההצמדה בפועל תתבצע בהתאם למועד פרסום המדד הרלוונטי. ככל שהתאריך הקובע אינו יום עדכון המדד, ביצוע ההצמדה יחל ביום עדכון המדד האחרון, הקודם לתאריך הקובע.

3.4. סכום ההצמדה שיחושב יתווסף או יופחת לתעריפים שנקבעו בהתקשרות.