משרד החוץ
ירושלים

אל: המציעים שנרשמו להשתתפות במכרז

כב' אלול, תשפ"ב
18/9/2022

נספח – דרישות הגנה בסייבר והגנת המידע

1. כללי

1.1 נספח זה מפרט את דרישות אבטחת המידע והגנת הסייבר של המזמין לפרויקט זה.

1.2 הספק אחראי לכלל היבטי אבטחת המידע והגנת הסייבר לאורך כל מחזור החיים של הפתרון המוצע, לרבות למידע של המזמין במועד סיום ההתקשרות, כמפורט בהנחיות נספח זה.

1.3 למען הסר ספק, בכל מקום בו צוין "ספק" או "מציע", הכוונה לכלל שרשרת האספקה של הספק - הספק עצמו, כל ספק משנה, יועץ או גורם צד שלישי המעורב בפתרון או באספקת השירותים במסגרת ההתקשרות.

2. נאמן הגנת סייבר ואבטחת מידע

2.1 הספק ימנה נאמן הגנת סייבר ואבטחת מידע (להלן "הנאמן") מצוות אבטחת המידע של הספק ובעל הכשרה מתאימה, האחראי על הגנת סייבר ואבטחת המידע הנכלל במאגרי המידע של המזמין, המאוחסנים במערכות ובשרתי הספק כנדרש על פי כל דין.

2.2 הנאמן יעמוד בקשר שוטף עם ממונה הגנת הסייבר של המזמין (להלן "מנהל הגנת הסייבר"), ויהיה אחראי על יישום הנחיותיו.

2.3 הנאמן יהיה בעל ניסיון, ידע והסמכות מתאימות וישמש כבעל מקצוע מרכזי לעבודה שוטפת מול מנהל הגנת הסייבר (POC), לרבות בשלבי התכנון, האפיון, ההקמה, ההטמעה, התפעול השוטף, התחזוקה, טיפול באירועי אבטחת מידע והגנת סייבר ושיפור מתמיד של מנגנוני אבטחת המידע והגנת הסייבר.

2.4 בעת ביקור נציגי המזמין במתקני הספק, ייפגש הנאמן עם מנהל הגנת הסייבר של המזמין.

3. עמידה בחוקים, תקנות, הוראות אסדרה (רגולציה) ואכוונה (מדיניות ותקני הגנת סייבר ואבטחת מידע)

3.1 הספק נדרש לעמוד בהוראות החוק החלות במדינת ישראל ובכל מדינה אחרת בה יסופק השירות.

3.2 הספק נדרש לעמוד בדרישות האסדרה (רגולציה) החלות במדינת ישראל ובכל מדינה אחרת בה יסופק השירות.

3.3 הספק נדרש לעמוד בדרישות האכוונה (קוים מנחים לרכש ומימוש) החלות במדינת ישראל מטעם התקשוב הממשלתי (בדגש על "נימבוס") ובכל מדינה אחרת בה יסופק השירות.

3.4 ספק השירות והיצרן נדרשים לעמוד בכל התקנים הבאים:

3.4.1 CSA STAR

3.4.2 ISO/IEC 27001

3.4.3 ISO/IEC 27701

3.4.4 ISO/IEC 27017

3.4.5 ISO/IEC 27018

3.4.6 ISO 22301

3.4.7 GDPR

3.4.8 AICPA SOC 1-3

3.4.9 PCi-DSS

3.4.10 HIPAA

3.4.11 NIST SP800-171

3.4.12 NIST CSF 1.1

3.4.13 NIST 800-53 (Rev. 4) או מקביל

3.4.14 תקן בינלאומי מוכר לניהול מהימנות עובדים

3.5 הספק נדרש לעמוד בבדיקות קבלה אבטחתיות לארכיטקטורה שנקבעה, סקרי סיכונים ומבדקי חדירה (Penetration Tests) עיתיים, אשר יאושרו על ידי מנהל הגנת הסייבר ומערך הסייבר הלאומי.

3.6 מתודולוגיה:

3.6.1 מסמכי מדיניות (ככל וישנם) - מדיניות להגנת המידע (InfoSec Policy), מדיניות הגנה (Cyber Defense Policy), מדיניות להגנת הפרטיות (Privacy Policy).

3.6.2 גבולות גזרה ותחומי אחריות בין נותן השירות למקבל השירות.

3.6.3 מדיניות ניהול זהויות, בקרת גישה (הזדהות) והרשאות {תיאור יכולות בקרת גישה וניהול משתמשים (User Management Procedure) }, לרבות תהליך וטכנולוגיות תומכות בהזדהות משתמשים (Authentication), לרבות נהלי פתיחה וסגירת חשבונות משתמשים (User Account Life Cycle) ואופן אבטחת חשבונות משתמשים ומנהלנים.

3.6.4 מדיניות הפרדת ישויות ברמת משתמשים וברמת אזורי פעולה תשתיתיים, אפליקטיביים ומידע (S.O.D).

3.6.5 מדיניות תיעוד, ניטור ובקרה (Audit Policy) ואופן שיתוף עם הלקוח.

3.6.6 אופן עמידה ברגולציה של הגנת פרטיות {רמת העמידה בכלל היבטי הגנת הפרטיות (הן בהיבטי התקנות הישראליות והן בהיבטי GDPR ותקנות פדרליות אמריקאיות)}.

3.6.7 פירוט אופן הטיפול במידע גיאוגרפי/ איכון ואישי.

3.6.8 אופן עמידה בניהול חולשות והקשחות אפליקטיביות ותשתיתיות.

3.6.9 אופן עמידה בהיבטי פיתוח מאובטח.

3.6.10 סקרי סיכונים ומבדקי חדירות/חוסן ככל שבוצעו.

4. <u>ארכיטקטורה וגבולות</u>

4.1 בשלב הכנת ההצעה, יעביר המציע למזמין מסמך המתאר את הארכיטקטורה המלאה של המערכת המתוכננת לספק את השירותים הנדרשים ואת הצעתו להגדרת גבולות האחריות בין הספק למזמין.

4.2 בשלב תכנון המערכת, יועברו לספק הנחיות לאבטחת המידע והגנת הסייבר מטעם מנהל הגנת הסייבר ומערך הסייבר הלאומי.

4.3 ההנחיות יכללו דרישות טכניות ונוהליות ליישום במערכת (לדוגמה: הזדהות חזקה, מימוש מנגנוני הצפנה מלאים, שילוב רכיבי חומת אש, סינון פוגענים ואנומליות, יכולות ניטור ביטחוני עמוקות, קבלת הכשרה מקצועית של החברה בנושא היבטי סייבר של היישום, ניהול אירועי אבטחת מידע והגנת סייבר, כתיבת נהלים רלוונטיים, מתן תדרוך ביטחוני למשתמשי המערכת השונים, סקרי סיכונים ומבדקי חדירה תקופתיים).

4.4 ההנחיות יידונו במשותף והספק יגיש למשרד מסמך תכנון על (HLD) ותכנון מפורט (LLD) לאישור.

4.5 במהלך הקמת המערכת, הספק יממש את התכנון בליווי ופיקוח של המזמין, בהתאם למסמכי התכנון.

4.6 הבהרות ודגשים לארכיטקטורה מאובטחת:

4.6.1 באם מוצע שירות בענן – האם ע"ג AWS ו/או GCP? אם לא – נא לפרט (כולל הסכמים שיש עם ספק הענן).

4.6.2 יכולת ניהול הגנה והחלת מדיניות ארגונית (CASB).

4.6.3 אופן הקישוריות לארגון.

4.6.4 הגנת הפרימטר הארגוני, ככל שיש כזה, ואם אין אז אופן הגדרה כזו.

4.6.5 חלוקת אזורי השירות לאזורים מאובטחים (דומיינים, תשתיות, יישומים, פיתוח,,,).

4.6.6 ממשקים מאובטחים (ממשקים ברמת התקשורת, האפליקציה והמידע אפשריים – הן בגלישה והן בחיבור פרטי).

4.6.7 בדיקת מידע שנשמר במאגרי המידע של הארגון, לרבות טכנולוגיות תומכות בהגנת המידע בהיבטי פרטיות (יכולות התממה, ערבול, הסתרה והצפנה בהתייחס למידע ביצירה, בתנועה ובמנוחה).

4.6.8 גישה למידע ומערכות תומכות מתוך הארגון ומחוצה לארגון ברמת משתמש, מנהלן, הגנת סייבר.

4.6.9 תהליכים/מדיניות גיבוי ושחזורים (Back Up And Recover Policy)

4.6.10 צורך במוצרי צד ג' (כדוגמת תשתית MDM ארגונית) ומדיניות עבודה עם צדדים שלישיים (External Party Management).

5. <u>הנחיות לתכנון הגנת הסייבר (כולל הגנת המידע)</u>

5.1 בשלב תכנון המערכת, יועברו לספק הנחיות לאבטחת המידע והגנת הסייבר מטעם המזמין ומערך הסייבר הלאומי.

5.2 ההנחיות יכללו דרישות טכניות ונוהליות ליישום במערכת, לרבות:

5.2.1 הנחיות לפיתוח מאובטח, לרבות תהליכי CICD.

5.2.2 דרישות אינטגרציה בהיבטי הגנת סייבר ואבטחת מידע.

5.2.3 הפרדת סביבות - פיתוח, בדיקות, ייצור.

5.2.4 הזדהות חזקה לרבות אמצעים פיזיים וכן התממשקות לתשתיות הזדהות חיצוניים.

5.2.5 ממשקים לתשתיות ארגוניות כגון: Active Directory, שרתי Exchange.

5.2.6 מימוש מנגנוני הצפנה מלאים.

5.2.7 הגנה אפליקטיבית.

5.2.8 ניהול זהויות ובקרת הרשאות.

5.2.9 שילוב רכיבי חומת אש תשתיתיים ואפליקטיביים.

5.2.10 סינון פוגענים ואנומליות.

5.2.11 יכולות ניטור אבטחתי עמוקות.

5.2.12 קישור ממוכן למערכות הניטור האבטחתי המרכזיות של המזמין.

5.2.13 זיהוי ומניעת דלף מידע.

5.2.14 אחסון, גיבוי ושרידות.

5.2.15 הגבלות על המיקום הגאוגרפי של מאגרי המידע.

5.2.15.1 אופן מניעת ניצול חולשות במערכים של הארגון.

5.2.15.2 ביצוע הקשחות עפ"י מדיניות הארגון (מדיניות הקשחות (Hardening Policy) במידה ומנוהל ע"י הספק).

5.2.15.3 מימוש עדכוני אבטחה עפ"י מדיניות.

5.3 ההנחיות יידונו במשותף והספק יגיש למשרד מסמך תכנון על (HLD) ותכנון מפורט (LLD) לאישור.

5.4 במהלך הקמת המערכת, הספק יממש את התכנון בליווי ופיקוח של המזמין, בהתאם למסמכי התכנון.

5.5 הספק יספק מערכת בקרות למזמין המאפשרת למזמין לבצע ניטור מהיכן בוצע חיבור למערכת.

5.6 הספק יערוך מבדקי חדירה וסקרי סיכונים לפחות אחת לשנה. תוצאות הסקרים והמבדקים יוצגו למזמין לרח״ט מתודולוגיות סייבר של המזמין בפגישה השנתית. על הספק להציג תכונית לתיקון הממצאים במידה ויש. במקרה של ליקויים מהותיים המשפיעים ישירות על מערכות המזמין משרד החוץ יש לידע באופן מידי את לרח״ט מתודולוגיות סייבר של המזמין על המצאות הליקוי.

6. ניהול משתמשים והרשאות

6.1 הספק נדרש לנהל את הגישה לשירות הענן לפי סוג ההתקן (מחשבים נייחים/ניידים, טלפונים חכמים וכו׳) ומיקומו הגיאוגרפי.

6.2 תשתית המערכת המוצעת תכלול מערך ניהול זהויות והרשאות המאפשר את הגדרת יכולות הצפייה, העדכון, השליטה והבקרה של כל משתמש ובכל אובייקט.

6.3 יש להגדיר הרשאות גישה למידע באופן פרטני תוך הענקת הרשאות גישה רק לגורמים אשר גישתם למידע הכרחית לצורך מילוי תפקידם (לדוגמה ע״י מנגנון IAM).

6.4 הספק יאפשר שימוש במערכת ניהול המשתמשים של המזמין או במערכת SCIM לניהול זהויות והרשאות משתמשים, עפ״י החלטת המזמין.

6.5 הפתרון יתמוך בתהליכי ניהול משתמשים של המזמין, כגון קליטה ועזיבה של עובד, מעבר תפקיד, הוספת תפקידים ופרופילים וכדומה.

6.6 מנגנון ניהול המשתמשים וההרשאות, לרבות הקישור בין מערכות המשרד לבין הענן, יאופיין ע״י הספק בהתאם להנחיות מנהל הגנת הסייבר ומערך הסייבר הלאומי, בשלבי התכנון של הפרויקט.

7. בקרת גישה

7.1 על הספק לתמוך בהזדהות בשיטת MFA ע״י לפחות שניים מרכיבי ההזדהות הבאים:

7.1.1 Something you know: סיסמה מורכבת וארוכה. מענה זמני בלבד.

7.1.2 Something you have: כרטיס חכם, RSA Token, OTP, קוד הנשלח באמצעות SMS או מופק דרך טלפון/התקן חכם אחר.

7.1.3 Something you are: אמצעי ביומטרי כגון טביעת אצבע, רשתית עין, זיהוי פנים וכדומה.

7.2 מדיניות הסיסמאות תקבע ע״י מנהל הגנת הסייבר, בהתאם לתפקיד/פרופיל משתמשים, ותכלול הגדרה של מורכבות הסיסמאות, תוקף, הגבלות על שימוש

בסיסמאות היסטוריות, נעילת חשבון אחרי מספר ניסיונות הזדהות שגויים, פרק זמן לניתוק תקשורת (Session Time Out) המחייב זיהוי מחדש של המשתמש, ועוד.

8. <u>הגנת מידע בתנועה</u>

8.1 הספק נדרש להעביר מידע אשר נמצא בתנועה כגון מידע העובר בין המזמין לבין הענן, בין ספקי ענן שונים או בין רכיבים שונים בתוך הענן, על-גבי תווך תקשורת מוצפן לפחות אחד בתקן/שיטה מקובלים, אשר יאושרו ע"י מנהל הגנת הסייבר (כגון SSL, IPSEC, VPN, SSH וכו').

8.2 על הספק לתמוך בפרוטוקול המאפשר גישה למאגרי מידע פנימיים ליצירת שאילתות וביצוע עדכונים ללא צורך בשמירת המידע בענן (כדוגמת OData). הגישה למאגרי המידע תאובטח על-ידי פרוטוקול הזדהות כדוגמת OAuth 2.0, User Managed Access (UMA) או XACML.

8.3 הספק יידרש לאבטח את המערכת בענן באמצעים להגנה מפני מתקפות זמינות מסוג DDOS תשתיתי ואפליקטיבי.

8.4 הצעת הספק תכלול פתרון הגנת סייבר ואבטחת מידע בעל יכולות מתקדמות של ניטור ובקרה, מניעת פעילות זדונית בזמן הזיהוי, הצפנה במנוחה/תנועה, יכולות תיעוד ומעקב אחר פעולות ושינויים ויכולות אבטחה נוספות הנכללות בפלטפורמה זו.

9. <u>אבטחת נתונים נייחים</u>

9.1 הספק מתחייב לאחסן את נתוני המידע של המזמין בשיטה המאפשרת לפצל את המידע המאוחסן בשרתי הספק בין מספר שרתי אחסון שונים (כדוגמת מנגנון IDA), במטרה להקשות על תוקף או עובד הספק, בהשגת המידע בשלמותו.

9.2 הספק יאפשר למזמין להצפין מידע רגיש השמור בענן תוך שימוש באלגוריתם הצפנה סטנדרטי ומוכר.

מידע רגיש הינו מידע המוגדר כרגיש על פי הוראת כל דין, או שהוגדר כך על-ידי קב"ט המזמין, או על-ידי מנהל הגנת הסייבר של המזמין.

9.3 יש לפרט יכולות מניעת דלף מידע ושליטה במידע (יכולות הצפנה, הסתרה, ערבול, האפלה וכדומה) והגנה על המידע במנוחה בתנועה ובעיבוד (in Motion, in Process & at Rest).

9.4 הספק יאפשר למזמין לערפל (Obfuscation) להתמים/ להסתיר (Anonymization\ Masking) ו/או לערבל ו/או להצפין מידע ביצירתו, שינוע/ עיבודו ואחסונו בענן על-פי דרישת המזמין בכל עת.

9.5 הספק יתמוך באפשרות ששדה מהותי אחד לפחות (שדה מזהה המאפשר זיהוי חד ערכי) יאוחסן ברשת המזמין ולא ברשת הספק.

9.6 הספק יתמוך בהצפנה תוך שימוש במערכת HSM כך שיאפשר למזמין לשמור מפתחות הצפנה אשר יהיו בשליטה בלעדית של המזמין (חילול והחלפת מפתחות). לספק לא תהיה גישה למערכת ה-HSM, למעט לצורכי הצפנת מידע.

9.7 על הספק להציג בפני מנהל הגנת הסייבר את ארכיטקטורת אחסון הנתונים בענן, כדי לאפשר למזמין לזהות סיכונים אבטחתיים ולקבוע בקרות זמינות להתמודדות עם סיכונים אלו, אשר הספק יהיה מחוייב ליישם.

10. <u>תקשורת והתקני קצה</u>

10.1 הספק יתמוך בקישור למערכות המזמין בשתי החלופות הבאות:

10.1.1 דרך האינטרנט בתווך מוצפן.

10.1.2 באמצעות תשתית ייעודית מוצפנת בין הספק למזמין אשר תאפשר רציפות עבודה במידה והגישה לספק דרך רשת האינטרנט לא תתאפשר.

10.2 הספק יאפשר ניתוב (routing) בין תקשורת האינטרנט לבין התשתית הייעודית.

10.3 הספק יספק אפשרות כניסה לענן מבוסס מיקום וכתובות IP.

10.4 הספק יאפשר למזמין להגדיר מדיניות לזיהוי משתמשים והתקני קצה, לרבות הגבלת מיקום גיאוגרפי, סוג התקן ושייכותו הארגונית, ויאכוף מדיניות זו כחלק אינטגרלי מהשירותים אותם יספק.

11. <u>ניהול מפתחות הצפנה</u>

11.1 הספק יאפשר למזמין לנהל את מפתחות ההצפנה באופן עצמאי במתקני המזמין או על-ידי גורם צד שלישי המתמחה בניהול מפתחות הצפנה, עפ"י החלטת מנהל הגנת הסייבר.

11.2 אם יוחלט כי ניהול מפתחות ההצפנה יבוצע בענן, על הספק לספק רכיב ייעודי לאחסון וניהול מפתחות הצפנה באופן מאובטח, בהתאם לדרישות מנהל הגנת הסייבר.

11.3 הספק יעמוד בתקני אבטחה מחמירים כגון FIPS 14-2, Common Criteria EAL4+ וכדומה, ויתמוך בפרוטוקולי הצפנה סטנדרטים ומוכרים.

12. <u>שמירת המידע</u>

12.1 הספק יהיה מחויב לשמירת פרטיות הנתונים, בהתאם להנחיות המחייבות במדינה בה ממוקם מתקן המחשב ממנו מסופק השירות.

12.2 המזמין יהיה רשאי להורות כי נתונים שדות רגישים לא ישמרו במערכות הענן אלא במערכות המזמין.

12.3 האתרים בהם ישמור היצרן את המידע ימוקמו במדינת ישראל או במדינות הנכללות בהנחיות מנהל הגנת הסייבר.

12.4 היצרן יתחייב כי הנתונים שינוהלו ביישומים שיופעלו בעבור המזמין יוותרו בתחומי המדינות הנ"ל, ולא יועברו למדינות אחרות, בכלל זה לא יאגרו ע"י ספקי אינטרנט, סלולר וכו'.

12.5 היצרן מתחייב שלא להעביר המידע של המזמין לצד שלישי או לכל גורם אחר ללא הרשאה בכתב של המזמין.

12.6 היצרן יפעיל לכל הפחות שני אתרים, הממוקמים במרחק של מעל ל-100 קילומטר אחד מהשני, כאשר שני האתרים פועלים בגיבוי הדדי, וכל אחד מהם יכול לספק מענה מלא לכל צורכי המזמין, בכפוף להגדרת המדינות המאושרות לעיל.

12.7 היצרן מתחייב לאפשר למזמין לבצע בקרה על המידע השמור באתריו הפיזיים.

12.8 היצרן מתחייב למחוק את כלל המידע הקשור למזמין במסגרת הסכם זה עם תום ההתקשרות או בהתאם להנחייה של המזמין, ללא יכולת אחזור.

12.9 נדרש לפרט את אופן בדיקת מידע שנשמר במאגרי המידע של הארגון, לרבות טכנולוגיות תומכות בהגנת המידע בהיבטי פרטיות (יכולות התממה, ערבול, הסתרה והצפנה בהתייחס למידע ביצירה, בתנועה ובמנוחה).

12.10 נדרש לפרט את אופן הגישה למידע ומערכות תומכות מתוך הארגון ומחוצה לארגון ברמת משתמש, מנהלן, הגנת סייבר.

13. <u>אחסון וגיבוי</u>

13.1 מנהל הגנת הסייבר יקבע היכן יישמרו מאגרי המידע של המזמין לרבות אתר הגיבוי, לאחר המלצה של הספק ובהתאם לאמור בנספח זה.

13.2 הספק יפעיל גיבויים אוטומטיים בזמן אמת של מידע של המזמין בכל אתר בו הוא מאוחסן.

13.3 הספק ישמור גיבוי OFFSITE באתר שיאושר מראש ע"י מנהל הגנת הסייבר.

13.4 שיחזור מידע והעלאת נתונים מגיבוי הינם באחריות ניהול ותפעול של הספק.

13.5 הספק מחוייב לדווח למנהל הגנת הסייבר על כל פעולה של שיחזור מידע מגיבוי.

14. <u>אירועי אבטחת מידע וסייבר</u>

14.1 אירוע אבטחת מידע וסייבר מוגדר כאירוע בו קיים חשש להתרחשות נזק למזמין או לפגיעה בסודיותם, שלמותם וזמינותם של נכסי מידע של המזמין או לפגיעה בפרטיות כהגדרתה בחוק, ברגולציות או בתקנים המחייבים במסגרת ההתקשרות עם הספק.

14.2 המציע יפרט את נהלי התגובה לאירועי אבטחת מידע, הגנת סייבר ופרטיות (Security Incident Response) לרבות הענקת Admin/Security Console למזמין.

14.3 הספק מחוייב לדווח בזמן אמת למנהל הגנת הסייבר על כל חשד לאירוע אבטחת מידע או סייבר או אירוע חריג במתקניו העלול להצביע על חשד כזה.

14.4 האחריות לטיפול באירועי אבטחת מידע וסייבר הינה של הספק, בהתאם למתודולוגיות מוכרות (כבסיס – NIST), למחויבויות הספק במסגרת ההתקשרות, לתקני אבטחת המידע אליהם הוסמך הספק ובכפוף להנחיות פרטניות מטעם מנהל הגנת הסייבר של המזמין, ככל שיינתנו.

14.5 הספק יעביר בסוף כל חודש דוח מפורט, מאושר מטעם הספק ע"י נאמן אבטחת המידע, על אירוע אבטחת מידע וסייבר שזוהו וטופלו על ידו במהלך החודש החולף, ניתוח האירוע, הממצאים, המסקנות, הלקחים והצעדים שננקטו בעקבות האירוע.

14.6 יש לפרט יכולות ואופן קבלת מידע מהשירות/ תשתית הארגון בענן למערך ניטור בארגון המזמין.

15. <u>רישוי וגרסאות תוכנה</u>

15.1 הספק מתחייב להעמיד לרשות המזמין בזמן אמת את כלל יכולות ותכונות אבטחת המידע והסייבר בגרסאותיהם המלאות והעדכניות כחלק אינטגרלי מהפתרון.

15.2 כל מוצרי התוכנה בהם יעשה שימוש או בהם נדרש לעשות שימוש כחלק מהפתרון (כגון דפדפנים), נדרשים לתמוך בגרסאותיהם העדכניות ביותר.

16. <u>בדיקות הגנת סייבר ואבטחת מידע</u>

16.1 בדיקות הקבלה של המערכת יכללו בדיקות הגנת סייבר אבטחת מידע באמצעות סקרי סיכונים ממוקדים ולרבות מבדקי חדירה (Penetration Tests).

16.2 במהלך תקופת הבדק תחול על הספק אחריות בלעדית לתיקון/השלמת כל ליקויי הגנת הסייבר ואבטחת המידע שיתגלו, במועד הקצר ביותר האפשרי ובלוח זמנים שיוצג ע"י ספק למזמין ויאושר ע"י מנהל הגנת הסייבר.

16.3 סביבות הפיתוח, הבדיקות והייצור יהיו זהות בהיבטי יכולות הגנת סייבר ואבטחת המידע, לרבות עמידה בתקני הגנת סייבר ואבטחת מידע מחייבים.

17. <u>קורסים והכשרות</u>

17.1 הספק נדרש לקיים הכשרות בתחומי הגנת הסייבר ואבטחת המידע לעובדי המזמין הרלוונטיים, בדגש על מיצוי יכולות הפתרון להשגת הגנה אופטימלית.

18. <u>נגישות למידע על-ידי עובדי הספק</u>

18.1 הספק נדרש לעמוד בהנחיות מנהל הגנת הסייבר, הרשות להגנת פרטיות, מערך הסייבר הלאומי והתקשוב הממשלתי באשר להגבלת הנגישות של עובדיו למידע של המזמין.

18.2 אין לאפשר לעובד יחיד של הספק את היכולת לשלוף את כלל המידע של המזמין ; כל פעולה כזו מחייבת אישור פרטני של מנהל הגנת הסייבר, אשר יכלול זיהוי חזק שלו מול המזמין ואישור אקטיבי של הפעולה כתנאי לביצועה.

18.3 כלל הפעילויות מול בסיס הנתונים המרכזי ינוטרו ויתועדו ברמה פרטנית ובאופן חד ערכי.

19. פניית מגורם אכיפה לקבלת מידע

19.1 הספק מחוייב לעדכן על כל פניית גורם אכיפה מקומי או בינלאומי לקבלת נתונים של המזמין (עם או בלי צו בית משפט), טרם מסירת מידע כלשהו, וימנע ממסירת מידע של המזמין ללא אישור בכתב ומראש ע"י המזמין.

20. מניעת Lockdown

20.1 הספק יאפשר למזמין לשמור עותק מקומי של כלל המידע של המזמין בחצרות המזמין ו/או בכל אתר אחר שיקבע מנהל הגנת הסייבר וזאת על מנת למנוע מצב של Lockdown.

21. מעקב, ניטור ובקרה

21.1 הספק השירות יידרש לספק דוחות כגון SSAE16 SOC2 או ISAE3402 Type 2 report, אודות בקרות המיושמות בשטחו על-ידי גופים חיצוניים אמינים הסוקרים נושאים הקשורים להגנת הסייבר ואבטחת המידע, זמינותו, שלמותו וחשאיותו, לרבות בקרות הקשורות להגנה על הפרטיות עפ"י כל דין.

21.2 בהתאם למודל השירות הנבחר ולסוג המערכת או המידע הנשמרים בענן, על הספק להבטיח את אמינות נתוני הרישום של אירועים במערכות או ברכיבים שיוגדרו על-ידי מנהל הגנת הסייבר כבעלי רגישות גבוהה לתפקוד המערכת.

21.3 לצורך ניטור והתראה על אירועי אבטחה המתרחשים בענן, רישומי המערכת ייאספו על-ידי מערכת SIEM או Syslog ייעודית בענן ו/או ישלחו למערכת ה-SIEM של המזמין, בהתאם להחלטת מנהל הגנת הסייבר.

21.4 הספק יאפשר למזמין לאסוף את רישומי המערכת בזמן אמת/באופן מתוזמן.

21.5 לוגים יועברו בפורמט UTC.

21.6 הספק מתחייב לשמור היסטוריה של רישומי מערכת לתקופה המשתנה בהתאם לרגישות המערכת ולדרישות רגולטוריות התקפות למערכת, כפי שיקבע ע"י מנהל הגנת הסייבר.

21.7 על הספק לוודא כי רישומי המערכת נשמרים בשרת מרכזי המנוהל על-ידי צוות עובדים נפרד מהצוות המפעיל את המערכת.

21.8 אם הספק יבקש לשנות את מערכת הלוגים, עליו לעדכן את מנהל הגנת הסייבר 60 יום מראש, על מנת שיוכל להיערך.

21.9 הספק נדרש לבצע ניטור לשירותים ולמערכות בענן ברבדים הבאים:

21.9.1 ניטור לוגים – איתור בזמן אמת או בדיעבד של בעיות טכניות או אירועי הגנת סייבר ואבטחת מידע המתרחשים.

21.9.2 ניטור ביצועים – מעקב אחר עומסים במשאבי המחשוב בענן.

21.9.3 ניטור ומעקב אחר פעילויות חריגות/עויינות (ניסיונות הזדהות כושלים, גישה לא מורשית, ניסיונות כניסה כפולים ועוד).

21.10 הספק יספק מידע אודות תוצאות מבדקי חדירה המתבצעים במתקניו באופן תדיר לפי סטנדרטים מקובלים על פי תקני הגנת סייבר ואבטחת מידע.

22. <u>ביקורת – עמידה בהסכם בין הספק למזמין</u>

22.1 הספק יאפשר למנהל הגנת הסייבר ונציגים נוספים של המזמין, לקיים בכל עת סיור במתקניו הרלוונטיים לצורך ביקורת הגנת סייבר ואבטחת מידע ועמידה בהסכמים ו/או חוזים אשר יחתמו בין הספק למזמין. לכל סיור יצוותו הנציגים הרלוונטיים מטעם הספק על-פי דרישת המזמין, לרבות הנאמן.

22.2 אחת לשנה לפחות ייערך ביקור של נציגי המזמין במתקני הספק, בהתאם להחלטת המזמין.

22.3 הספק יאפשר למזמין להיפגש עם בעלי תפקידים רלוונטיים בתיאום מראש.

23. <u>סיום ההתקשרות עם הספק</u>

23.1 עם סיום ההתקשרות עם הספק, על הספק מוטלת האחריות לבצע את הנחיות מנהל הגנת הסייבר ומערך הסייבר הלאומי, לרבות הפעולות הבאות:

23.1.1 לפרט בהצעה תיאור תהליכי ביעור/ מחיקת מידע מהשירות עם סיום התקשרות.

23.1.2 מחיקה חד חד ערכית ולא ניתנת לשחזור של כל הנתונים והמידע השמורים בשירות הענן ונמצאים תחת שליטת המזמין.

23.1.3 השמדת עותקים של הנתונים והמידע בהם נעשה שימוש במסגרת פעילות הספק עבור המזמין.

23.1.4 דרישה מהספק להציג הוכחות לכך שהמידע הושמד (רישומים ודוחות רלוונטיים).

23.1.5 במקרים אחרים קבלה פיזית של רכיבי האחסון של המידע.

23.1.6 במידה והמידע הוצפן – ביטול (Revoke) מפתחות ההצפנה ומחיקתם.

24. נושאים רוחביים

24.1 מדיניות הביטחון:

24.1.1 מהימנות כ"א הפועל ישירות על הפרויקט לטובת המזמין יקבע בכפוף להנחיות גורמי הביטחון של המזמין.

24.1.2 היבטי ביטחון פיסי – כאמור לעיל.

24.2 נדרש לספק דוגמאות ל:

24.2.1 מסמך ניתוח סיכונים (Risk Analysis), לרבות מסמך ומדיניות הערכת סיכונים (Risk Assessment) לשירות המוצע.

24.2.2 תמונת מצב של ניתוח פגיעויות (Vulnerability Assessment).

24.3 אופן יישום תכן פרויקטלי – מסמכי תכנון (HLD, LLD וכדומה).