# הנחיות אבטחת מידע לספקים משרד הבריאות -

# מכרז מידענות

1.1. **כללי**

1.2. **בקרת גישה על המערכות**

1.3. **בקרת הרשאות**

1.4. **אבטחת תקשורת**

1.5. **הגנת תחנות קצה**

1.6. **ניהול משתמשים**

1.7. **אבטחה פיזית**

1.8. **הגנה על פריט מידע**

1.9. **גיבוי מידע**

1.10. **המשכיות עסקית**

**תנאי סף מקצועיים למציע:**

1. הספק ערוך ומתחייב להעמיד עבור המזמין שירות לפי דרישות מסמך זה גם בעת שעת חירום בהתאם ליעדי השירות המוגדרים בהסכם השירות (SLA), ובכלל זה יוגדר כמפעל חיוני לצורך הפעלת ריתוק משקי על עובדיו המעורבים במתן שירות.
2. הספק מתחייב שלא להקים מאגר נתונים ולא לשמור נתונים אודות מטופלים ולמחוק את המידע כולל ברשימות הלוגים ומכל מקום אחסון אחר לאחר חודש ממסירת המידע למשרד הבריאות או שמירת נתונים תבוצע על פי המתחייב בחוק. המזמין יוכל להאריך את משך שמירת המידע.
3. הספק מתחייב לאפשר למזמין \ מערך הסייבר או כל גורם אחר מטעמם לבצע בקרת אבטחת מידע בכל רגע נתון במעבדותיו.
4. הספק מתחייב לעדכן את המזמין בכל שינוי משמעותי בתהליך המחשוב, רשת ותקשורת הבדיקות.
5. הספק מתחייב שלא לעביר את המידע מחוץ לגבולות המדינה או למסור אותו לגורם אחר ללא רשות ממשרד הבריאות \ ארגון המבקש את הבדיקה.
6. הספק מתחייב שלא לבצע ולא לאפשר כל שימוש אחר בנתונים, זולת השימוש שהותר לו במסגרת חוזה ההתקשרות.

## 1. דרישות הסייבר

### 1.1. כללי

1.1.1. כל ספק הנותן שירותים בנושא המחשוב חייב לעמוד בדרישות המוגדרות בפרק זה.

1.1.2. מטרת הפרק להגדיר ולקבוע את ההוראות וההנחיות שיחייבו את הספק ואת כל מי מטעמו שיועסק במתן השירותים, כחלק מכלל הפעולות, הננקטות בכדי להגן על מידע של משרד הבריאות/ארגוני הבריאות.

1.1.3. האמור בפרק זה הינו תנאי מחייב לביצוע השירותים.

1.1.4. מוסכם ומוצהר כי ההתחייבויות שבסעיף זה, יעמדו בתוקפן גם במקרה של סיום או ביטול ההתקשרות לתקופה של 7 שנים מתום תקופת ההתקשרות בהסכם ההתקשרות.

1.1.5. עמידה בחוקים, תקנות והנחיות וחוזרי מנכ"ל המתפרסמים מעת לעת על ידי מנכ"ל המשרד, רמו"ט ומחלקת אבטחת מידע במשרד הבריאות.

1.1.6. הספק מחויב לעמוד בחוק הגנת הפרטיות התשמ"א – 1981 ולתקנות הגנת הפרטיות התשע"ז 2017.

1.1.7. ייעשה שימוש במגוון שיטות וכלים טכנולוגיים להבטחת שלמות ואמינות הנתונים המועברים בין רכיבים שונים של מערכת, בין מערכות בתוך הארגון (ממשק פנימי) ומהארגון החוצה (ממשק חיצוני).

1.1.8. הספק יהיה אחראי כלפי המזמין על כל המידע המועבר אליו או דרכו, לרבות דוחות, טפסים, קבצים מגנטיים, מידע לגבי נתונים אישיים ומערכות מידע של המזמין.

1.1.9. הספק ידאג לאבטחת כל חומר שיגיע אליו במסגרת ביצוע התחייבויותיו על פי מכרז זה, ויציג למזמין, על פי דרישתה, את אמצעי אבטחת החומר.

1.1.10. הספק יתחייב לשמור בסודיות מלאה כל נתון ו/או מידע שהגיעו אליו במסגרת ביצועו של חוזה ההתקשרות לביצוע פרויקט זה, בין במישרין ובין בעקיפין ולא יגלה כל נתון ו/או מידע כאמור לכל צד שלישי שהוא.

1.1.11. כמו כן מתחייב הספק לגרום לכך שכל המועסקים על ידו בביצוע הסכם ההתקשרות למתן שירות עבור המזמין יחתמו על התחייבות לשמירת סודיות. הספק יצהיר שידוע לו שאי מילוי התחייבויותיו לפי סעיף זה מהווה עבירה על פי חוק העונשין, התשל"ז - 1977 ועבירה על חוק הגנת הפרטיות, התשמ"א - 1981.

1.1.12. הספק אינו רשאי לעשות שימוש שלא לעניין מילוי מחויבויותיו בגין מכרז זה במידע מכל סוג שיגיע אליו במסגרת עבודתו, לרבות מידע אודות הציוד לסוגיו, מידע סטטיסטי אודות השירות וכל מידע אחר.

1.1.13. עם סיום ההתקשרות יחזיר הספק למזמין את כל החומר האמור, או ישמידו לפי הוראת המזמין.

1.1.14. הספק מתחייב לבצע פיתוח ככל שנדרש על פי נוהל הפיתוח המאובטח הארגוני ועל פי מתודולוגיית תכנון ופיתוח (כולל עמידה של אנשי צוות הפיתוח בתקנים ובדיקות) בצורה מאובטחת.

1.1.15. הספק מתחייב לעמוד בדרישות אבטחת המידע של משרד הבריאות כפי שהן מופיעות בנספחים המצורפים למסמך זה.

1.1.16. הספק ידאג לאבטחת כל המידע אשר יגיע אליו במסגרת מכרז זה. הספק אף יגן על המידע מפני כל נזק, לרבות גניבה, שריפה וכד'.

1.1.17. הספק ימנע גישה למערכות המחשב שברשותו, או למערכות המחשב המשרתות אותו לצורך מתן שירותי מכרז זה, ממי שאינו מוסמך לעיין בחומר או במידע

המאוחסן במחשב, או ממי שלא חתם על התחייבות לשמירת סודיות.

1.1.18. הכניסה למערכות המחשוב של משרד הבריאות תתבצע באמצעות גישת MFA מאובטחת באמצעות כרטיס חכם ו/או רכיב ביומטרי ו/או OTP ו/או PNA עפ"י החלטת המשרד. בכל מקרה, הספק ירכוש כרטיס חכם לכל היועצים העובדים מטעמו לצורך מתן שרות במסגרת ההתקשרות.

1.2. **בקרת גישה על המערכות**

1.2.1. <u>גישה למערכות המזמין</u>

1.2.1.1. אימות המשתמש בהתחברותו לשירות המזמין, יעשה באמצעות מערכות הגנה אפליקטיבית.

1.2.1.2. הזדהות המשתמש מול משאבי המזמין תהיה באמצעות MFA – סיסמה + כרטיס חכם ו/או רכיב ביומטרי ו/או OTP בתצורת Secured Desktop.

1.2.1.3. לצורך גישה למערכות המזמין הספק נדרש לרכוש כרטיסים חכמים מספקים המאושרים ע"י המזמין.

1.2.1.4. גישה אל משאבים הרלוונטיים של המזמין תינתן לעובדי ספק המורשים בלבד.

1.2.2. <u>גישה למערכות הספק</u>

1.2.2.1. לא תהיה אפשרות לגישה אנונימית למשאבי מידע של הספק.

1.2.2.2. בקרת גישה למערכות מידע תיושם עפ"י מהות התפקידים .

1.2.2.3. גישת המשתמש אל המערכות המידע לא תהיה ישירה אלא רכיבי הגנה, כדוגמת - Terminal Server, WAF, PROXY וכו' לפי העניין.

1.3. **בקרת הרשאות**

1.3.1. הרשאות למשתמשי המערכות תינתנה עפ"י עקרות "המינימום הנדרש" ( Least Privilage) בהתאם לאפיון התפקיד ובאישור בעל המידע בכל מערכת.

1.3.2. עם שינוי ו/או הסבת תפקידו של בעל החשבון כלל ההרשאות הקודמות יבוטלו וינתנו עפ"י הפרופיל החדש.

1.3.3. במקרה של סיום/הפסקת העסקה של עובד ו/או אצל הספק גישה למערות תחסם באופן מיידי

1.3.4. מתן כל **הרשאת גישה מותנית** בחתימת העובד על הצהרת שמירת הסודיות.

1.4. **אבטחת תקשורת**

1.4.1. <u>תשתיות תקשורת LAN</u>

1.4.1.1. כלל תשתיות תקשורת יופרדו ברמה פיזית ל-2 דומיינים IT – Information Technology ו-OT – Operational Technology.

1.4.1.2. חיבור ו/או התממשקות בין ה-IT ל-OT, ככל שנדרש, יהיה באמצעות רכיב

אבטחה ייעודי בשכבות גבוהות ודרך FW ייעודי.

1.4.1.3. הספק נדרש להפעיל מערכת הגנת בקרת גישה למשאבי רשת NAC לכלל מרכיבי הרשת, בתצורה של אכיפת "תביעת אצבע" לכל סוג רכיב.

1.4.1.4. תשתית פסיבית בתוך אתרי הספק לא תהיה חשופה לשוהים ומבקרים באתרים אלו ותושחל בצורה נסתרת בתוך קירות ו/או תעלות פח.

1.4.1.5. תשתית אקטיבית תמוקם בארונות תקשורת ייעודיים נעולים פיזית ובאופן שמונע אפשרות גישה לא מורשית לציוד.

1.4.2. כלל רשתות ה-LAN יופרדו זו מזו באמצעות FW.

1.5. **הגנת תחנות קצה**

1.5.1. מערכות הפעלה תהינה מתוחזקות, מעודכנות ומסונכרנות, בהתאם לפרסומים רשמיים של יצרניהן.

1.5.2. תחנות קצה יהיו מוגנות באמצעות מערכות EPS או מתקדמות יותר. עדכוני גרסאות ומקורות מידע יהיו מתוזמנות עם יצרניהן.

1.5.3. תחנות קצה ינוהלו ע"י הספק באופן מרכזי כולל ניהול סיסמאות, יהיו בדומיין בעל מדיניות הקשחה שבא למזער את חשיפת המשתמש לחולשות אבטחה ידועות ולא ידועות.

1.5.4. יישומים מובנים בתוך מערכת ההפעלה שלא נחוצים יחסמו.

1.5.5. דפדפני האינטרנט יוקשחו לפי המדיניות הארגונית.

1.5.6. אחר 15 דקות של חוסר שימוש, התחנה תינעל ותתאפשר כניסה רק לאחר הכנסת פרטי זיהוי

1.6. **ניהול משתמשים**

1.6.1. הקמת חשבון המשתמש עבור השרות, עדכונו וביטולו יבוצע ב-AD של הדומיין המקומי של הספק בקבוצה ייעודית עפ"י מדיניות ניהול המשתמשים של הספק.

1.6.2. במקביל, על הספק להגיש בקשה למזמין לצורך להקמת/גריעת חשבון המשתמשים במערכות הרלוונטיות של המזמין, ככל שנדרש, לצורך מתן שרות. הנ"ל עפ"י נוהל ניהול משתמש של המזמין.

1.6.3. ניהול חשבונות משתמשים מסוג Local Admin יהיה מרכזי באמצעות Microsoft LAPS או דומה.

1.6.4. במקרה של סיום/הפסקת העסקה של עובד ו/או אובדן ו/או גניבה של כרטיס חכם של העובד המורשה, מנהל האתר או בר כוחו יהי אחראי לביצוע ותיעוד, בין היתר, את הפעולות הבאות:

1.6.4.1. דיווח מידי למזמין ולמנהל המערכת על המקרה, לצורך ביטול חשבון המשתמש במערכות המזמין.

1.6.4.2. לפנות לגורם שהנפיק את הכרטיס החכם ע"מ לבצע Revocation של התעודה.

1.6.4.3. לוודא באופן פרונטלי את גריסת הכרטיס החכם תוך ביצוע תיעוד על כך.

1.7. **אבטחה פיזית**

1.7.1. <u>אחריות</u>

1.7.1.1. עובדי הספק יהיו אחראים על ליווי אורחיהם ותשומת לב לאורחים לא קרואים.

1.7.1.2. באזורים רגישים, על מנהל האתר לוודא קיומן של הבקרות הבאות:

1.7.1.2.1. קירות חיצוניים מוצקים וכל הדלתות החיצוניות מוגנות היטב בפני גישה בלתי מורשית, באמצעים כגון: מנגנוני בקרה, מנעולים ומערכות אזעקה.

1.7.1.2.2. דלתות בקרת אש על פי דרישות תקן הבטיחות.

1.7.1.2.3. מחסומים פיזיים באזורים המכילים ציוד מחשוב רגיש, כדי למנוע כניסה בלתי מורשית וסכנות סביבתיות העלולות להיגרם כתוצאה משריפה או הצפה.

1.7.1.2.4. חלונות חדר המחשב ו/או תקשורת יהיו מסורגים וסגורים באופן שתהייה הגנה על זגוגיות החלון מפני ניפוץ, ובנוסף תותקן מערכת אזעקה.

1.7.1.2.5. באזורים רגישים יהיו אמצעי כיבוי אש כגון: מטפים, מערכות התזת מים ומערכות גילוי עשן.

1.7.1.3. שרתי המערכת ויתר ציוד הליבה יגובו מפני הפסקות חשמל באמצעות מערכות אל פסק.

1.7.1.4. תותקן תאורת חירום במקומות מרכזיים אשר תפעל בעת הפסקת חשמל.

1.7.2. **אבטחת משרדים, חדרים ומתקנים**

1.7.2.1. חדרים המכילים מידע ינעלו בעת היעדרות העובד מחדרו ובעזבו את החדר בסיום יום העבודה.

1.7.2.2. כל מידע רגיש בהיבט עסקי או של צנעת הפרט ישמר בארון נעול או בכספת כל עוד לא נעשה בו שימוש או כאשר העוסק בו אינו בקרבתו.

1.7.2.3. חדרים המכילים חיווט או ציוד תקשורת כגון ארונות חיווט ומערכות טלפוניה יהיו נעולים תמיד והגישה אליהם תוגבל לעובדים מורשים בלבד.

1.7.2.4. דלתות האזורים הרגישים יהיו נעולות תמיד. כניסה לגורם מאושר תתאפשר על ידי תג כניסה או מפתח.

1.7.2.5. לא יהיה סימון המשמש אינדיקציה למיקום מחשבים או מרכזי תקשורת על מנת לא למשוך את תשומת ליבם של בלתי מורשים.

1.8. **גיבוי מידע**

1.8.1. הספק נדרש לגבות את כל המערכות המעורבות במתן שירות למזמין בתוך גבולות של מדינת ישראל.

1.8.2. אופן הגיבוי למערכות מידע ייקבע ע"י מדיניות גיבויים של הספק ומבלי לפגוע מדרישות מסמך זה.

1.8.3. כל יום יבוצע גיבוי למידע.

1.8.4. באתרים בהם מבוצעים גיבויים דיפרנציאליים או אינקרמנטליים, יבוצע בכל מקרה גיבוי מלא לפחות אחת לשבוע.

1.8.5. גיבוי למערכות קריטיות בין היתר יהיה גיבוי חם, קרי - זמינות מידית.

1.8.5.1. .

1.8.6. עותק של הגיבוי הרבעוני יוחזק באופן מאובטח באתר מרוחק (אתר DR) מהאתר בו ממוקמות מערכות.

1.8.7. עותק של גיבוי חודשי יועבר באופן מאובטח לרשות המזמין ויוחזק באתר שלו.

1.9. **המשכיות עסקית**

1.9.1. כתנאי מקדים להפעלת פעילות הספק יגיש לאישור המזמן את תכנית המשכיות עסקית שכוללת לפחות נושאים הבאים:

1.9.1.1. **משאבי אנוש** - בהתבסס על ניתוח ההשלכות העסקיות, יוגדרו תחומי האחריות והסמכות, לחברי ההנהלה, צוותי עבודה, נותני שירותים פנימיים וחיצוניים , וגורמים אחרים. כמו כן, תיבנה תכנית גיבוי לכ״א חיוני ויוגדר צוות מקצועי לניהול והפעלת התהליכים והשירותים החיוניים בעת חירום, לרבות במקרה של שביתה, אסון טבע, אירוע בטחוני, מגפה ו/או פנדמיה וכיו״ב.

1.9.1.2. **נושאים טכנולוגיים** - תכנית ההמשכיות העסקית תתייחס לכל מרכיבי הטכנולוגיה הנדרשים לשמירת הרציפות העסקית ו/או לאישוש הפעילות.

1.9.1.3. **העתקת תהליך או שירות חיוני** - תכנית המשכיות העסקית תיתן ביטוי להעתקת תהליך או שירות חיוני למיקום חדש.

1.9.1.4. **חלופות עבודה ידנית** - תכנית ההמשכיות העסקית תכלול, בהתאם לעניין, נהלים לביצוע תהליכי עבודה ידניים, אשר אושרו מראש על ידי הנהלת הספק ,כחלופה לתהליכים ושירותים חיוניים. בהקשר זה, הספק ידאג לגיבוי רשומות מידע של המזמין.

1.9.1.5. **גיבוי נתונים** – כמפורט בסעיף 1.9 לעיל.

1.9.1.6. **תקריות אבטחת מידע** - תפותח מדיניות תגובה לאירועי אבטחת מידע אשר תשולב בצורה נאותה בתכנית ההמשכיות העסקית. במקרה של פריצת מעגלי ההגנה, אלמנט מרכזי בתגובה לאירוע אבטחת מידע הוא חלוקת האחריות להערכה, לתגובה ולניהול אירועי האבטחה ופיתוח קווים מנחים לעובדים בנוגע לנוהלי הסלמה ודיווח. הספק נדרשת לקבוע מי יהיה אחראי להכריז על תקרית, ומי אחראי לשחזר את מערכות המחשב שנפגעו מרגע שהתקרית הסתיימה. מי שמוטלת עליו אחריות זו צריך להיות בעל המומחיות הנדרשת כדי להגיב בדרך מהירה ונאותה

1.9.1.7. **מדיניות ״גישה מרחוק״** - נהלי עבודה לגישה מרחוק יהיו חלק מתכנית ההמשכיות העסקית, שכן באירועי חירום מסוימים לא תתאפשר גישה לחלק ממתקני הספק, ולכן עלול לעלות צורך במתן גישה מרחוק לעובדים או נותני שירותים חיצוניים. מדיניות הגישה מרחוק תאושר ע״י ההנהלה הבכירה ותתייחס לסיכונים הכרוכים במדיניות ולקיום מנגנוני בקרה ואבטחת מידע הולמים.