

נספח דרישות אבטחת מידע וסייבר - שירותי פיתוח ותחזוקה לתוכנות ומערכות

אוגוסט 2023 [נוסח מעודכן]

א. כללי

1. הספק ימנה נאמן אבטחת מידע וסייבר, שיהיה אחראי ליישום כלל היבטי אבטחת המידע במערכות ובתהליכים הרלוונטיים לשירות המסופק.
2. הספק מתחייב ליישם את דרישות "תורת ההגנה בסייבר לארגון" של מערך הסייבר הלאומי תוה"ג 2.0 באופן שהולם את פעילותו, גודלו ומורכבותו, ותוך ניהול הסיכון כפונקציה של הסתברות והשפעה.
3. תכניות העבודה ליישום הבקרות על-פי תורת ההגנה תאושרנה על-ידי נתיבי איילון.
4. הספק מתחייב לעמוד בתקן ISO27001.
5. ספק השירות יפעל על פי עקרונות [מסמך מדיניות פיתוח מערכת מאובטחת](#) של ממשל זמין.

ב. שמירת סודיות

1. הספק מתחייב לעמוד בהוראות חוק המחשבים, התשנ"ה 1995 הפרטיות, התשמ"א 1981 ותקנות הגנת הפרטיות (אבטחת מידע) ובכללם חוק הגנת התשע"ז.
2. היה וספק השירות מבצע שימוש בתשתית מחשוב של ספק אחר (ענן, Hosting) עליו לציין זאת ולצרף מסמך המתאר כיצד מתבצעת חלוקת האחריות בינו לבין ספק התשתית הנוסף ובאילו אמצעים הוא נוקט בכדי להגן על המידע ולאשרם מול גורמי אבטחת מידע וסייבר בנתיבי איילון.
3. הספק מתחייב למלא אחר כל הוראות אבטחת המידע לגבי שמירת מידע כפי שיועברו ע"י נתיבי איילון. [מובהר כי סעיף ב'3 זה כפוף להחלטות נתיבי איילון בקשר עם המכרז ולא להחלטות אחרות של נתיבי איילון שאינן קשורות.](#)
4. הספק ידאג לאבטחת כל חומר שיגיע אליו במסגרת ביצוע התחייבויותיו על פי הסכם זה ויהיה אחראי כלפי נתיבי איילון 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 נתיבי איילון.
5. באחריות הספק לדאוג לחיסיון, אמינות וזמינות המידע של נתיבי איילון שברשותו.
6. הספק יהיה אחראי לכל עקיפה או ניסיון עקיפת מנגנוני אבטחה ובקורות גישה לתשתיות שונות, שיבוצעו על ידי העובדים מטעמו.
7. בעת אירוע אבטחת מידע או אירוע חריג אצל הספק, בו קיים חשד לגבי דלף מידע של נתיבי איילון, הספק מחויב להודיע באופן מידי לאיש הקשר בנתיבי איילון.
8. הספק מתחייב לשתף פעולה עם נתיבי איילון בכל אירוע חריג או חשד לכזה אשר עלול להשליך במישרין אן בעקיפין על ביטחון ואבטחת המידע של נתיבי איילון.
9. כל מידע אשר יועבר לנתיבי איילון יועבר האופן מוצפן.
10. מידע מוגבל יהיה נגיש לעובדי הספק ע"פ עקרון Need to know\Need to do.
11. נתיבי איילון תהא רשאית לבצע ביקורות תהליכיות וטכנולוגיות בחצרות הספק לאחר תיאום איתו, הספק מתחייב לשתף פעולה עם נציגיה של נתיבי איילון לצורך כך.

ג. אבטחה פיסית

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.
2. אמצעים לבקרת כניסה פיסית: 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.
3. הספק מתחייב ליישם הגנה פיסית מפני נזקי שריפה, הצפה, תקלות מתח וכיו"ב.
4. הספק מתחייב לנקוט בכל הצעדים הרלוונטיים לאבטחת ציוד וניירת – ביו היתר, מחיקת מידע רגיש/סודי ואף השמדת המדיה, גריסת והשמדת ניירת.
5. הספק מתחייב כי כל כניסת לקוחות/ספקים לאזורי השרתים תהיה מבוקרת ומתועדת.

אבטחה לוגית

1. הספק מתחייב ליישם אמצעי אבטחה הולמים שימנעו חדירה מכוונת או מקרית למערכת או למערכות התשתית והתקשורת, יש לפרט במענה את אמצעי הבקרה שהספק מציע.
2. הספק מתחייב לבצע הפרדה בין רשתות המאכלסות את מאגרי המידע של נתיבי איילון ליישומים ולכלל הרשתות (סגמנטציה) באמצעות הפרדה לוגית הכוללת סגמנט מבודד מאחורי חומת אש (FW).
3. הספק מתחייב כי אמצעי אבטחת המידע שברשותו יעברו הקשחות לפי המלצות היצרן ו – Best Practices ידועים.
4. הספק מתחייב לעדכן באופן שוטף את המערכות השונות למניעת ניצול פרצות אבטחת מידע.
5. הספק מתחייב שמערכות אבטחת מידע יספקו שרידות מלאה לשמירה על זמינות המערכת.
6. הספק מתחייב לדאוג לגישה ממודרת על בסיס הגדרת תפקידים.
7. במידה וקיבל הספק אישור וחיבר את המערכות ו/או מאגרי המידע לרשת ציבורית או לאינטרנט, מתחייב הספק 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 הבקורות והאמצעים הנותנים מענה לדרישה.
8. הספק מתחייב שהעברת המידע בתוך רשת התקשורת, ברשת ציבורית או על גבי רשת האינטרנט תיעשה תוך שימוש בשיטות הצפנה מקובלות.

ד. מנגנון תיעוד ובקרה

1. הספק מתחייב לנהל מנגנון תיעוד אוטומטי שיאפשר בקרה וביקורת על מערכות שניגשות למאגרי מידע של נתיבי איילון, יש לצרף למענה את הפתרון לדרישה.
2. על הספק לבצע תיעוד של כל אירוע אשר יש בו משום פגיעה בשלמות, סודיות וזמינות המידע, יש לצרף למענה את הפתרון לדרישה.
3. כל אירוע אבטחה, ייחקר וייבדק ויופק דוח אירוע המתאר את הגורמים לאירוע ואת דרכי הטיפול באירוע. הספק יוציא הנחיות לביצוע על מנת להפחית את הסיכוי לאירוע דומה.
5. על הספק להכין הוראות להתמודדות עם אירועי אבטחת מידע אשר מתייחסים לחומרת האירוע ולמידת רגישות המידע. בהוראות אלו תהיה התייחסות לצעדים מידיים הנדרשים לטיפול באירוע כגון דיווח לנתיבי איילון, ביטול הרשאות וכדומה, יש לצרף למענה דוגמא לדרישה.

6. הספק ישלב פתרון לתיעוד פעילות אשר תוגדר קריטית במערכת, פעילות אשר נראית חריגה (כולל פעילות בבסיס הנתונים ו/או במערכת ההפעלה) ופעילות או ניסיונות לביצוע פעולות אשר נוגדת ישירות את המדיניות שהוגדרה במערכת. כמו כן, על המערכת לספק כלים מתאימים לשמירה על קבצים אלו ויכולות דיווח לבעלי התפקידים המתאימים כדי שיוכלו לטפל בהתרעות.

ה. ניהול משתמשים והרשאות

1. הספק מתחייב שגישה למערכות המידע ו/או מאגרי המידע תהיה מבוססת על בסיס הצורך לדעת (need to know) ולא תורשה גישה מעבר לנדרש לצורך מילוי התפקיד כפי שהוגדר על ידי נתיבי איילון ובהתאם להוראות המכרז.
2. הספק מתחייב לדאוג לגישה ממודרת על בסיס הגדרת תפקידים. הספק מתחייב לנהל רישום מעודכן של בעלי התפקידים ושל הגישה המוגדרת לכל תפקיד.
3. הספק מתחייב לגרוע הרשאות לבעלי תפקידים שהסתיים תפקידם או שאין להם צורך במידע אליו קיבלו הרשאה.
4. הספק מתחייב לדאוג לבקורות המתאימות על מנת שלא תבוצע גישה לא מורשית למאגרי המידע, יש לצרף למענה את הפתרון לדרישה.
5. הספק מתחייב שהזדהות לניהול הרשת והשירותים הניהוליים מרחוק תבוצע באמצעות רכיב בנוסף לסיסמה - OTP. מובהר ביחס לרכיב לביצוע ההזדהות כי יהיה כל אמצעי/מנגנון otp - הודעת sms אפליקציית אימות של גוגל או מיקרוסופט וכיו"ב.
6. על הספק לזהות את המשתמשים במערכות שבמכרז, במערך ההזדהות תוגדר מדיניות סיסמאות ע"פ Best Practices ידועים.

ו. אבטחת רכיבי תקשורת

1. הספק מתחייב כי מערכות ומאגרי המידע של נתיבי איילון לא יחוברו לסביבת האינטרנט, אלא אם כן קיבל על כך אישור מראש מגורמי אבטחת המידע בנתיבי איילון.
2. במידה וקיבל הספק אישור וחיבר את המערכות ו/או מאגרי המידע לרשת ציבורית או לאינטרנט, מתחייב הספק 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 הבקורות והאמצעים הנותנים מענה לדרישה.
3. הספק מתחייב שהעברת המידע בתוך רשת התקשורת, ברשת ציבורית או על גבי רשת האינטרנט תיעשה תוך שימוש בשיטות הצפנה מקובלות.
4. על הציוד המשמש להעברת תקשורת (מתגים, נתבים, FW) לעבור הקשחות בהתאם להמלצות היצרן ולעבור עדכוני קושחה.
5. התשתיות והפלטפורמות יותקנו ע"י הספק תוך שימוש בתוכנות ורישיונות מקור בלבד. בשימוש בתוכנות יש לוודא בדיקת הלבנה לפני ההתקנה למניעת החדרת קוד עויין. בשימוש במערכות וירטואליות יש להתקין מחדש קובץ MASTER מהימן ובדוק.

ז. אבטחת עמדות קצה

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

2. רכיבים ושרתים לא יועברו מפרויקט אחד למשנהו, לא יעשה שימוש בציוד שנעשה בו שימוש שלא עבור הפרויקט, אלא באישור המשרד בלבד.
3. מחשבי הספק מהם ניתן לגשת למידע של נתיבי איילון ולמערכותיה, יצוידו במערכת הפעלה ובתוכנות אנטי וירוס/EDR מעודכנות לצורך הגנה מפני קוד זדוני (וירוסים, תולעים, סוסים טרויאנים, רוגלות ותוכנות זדוניות אחרות).
4. הספק מתחייב להתקין רכיב סינון תוכן (content filtering) אשר ימנע כניסה של קוד זדוני לרשת הספק בעת גלישה לאינטרנט ושימוש בדוא"ל אשר יאושר ע"י נתיבי איילון.
5. הסביבה שתוגדר לצורך טיפול במידע של נתיבי איילון תופרד מסביבת העבודה של הספק באמצעות אמצעים לוגיים (FW).
6. החיבור אל מערכות המידע של נתיבי איילון יהיה בהתאם להנחיות אשר יתקבלו מגורמי המחשוב ואבטחת המידע בנתיבי איילון.

ח. שימוש בהתקנים ניידים

1. הספק מתחייב שלא להוציא חלקי מידע להתקנים ניידים למעט גיבוי המידע כפי שנקבע על ידי נתיבי איילון.
2. במידה ונדרש מהספק לצורך פעילותו לבצע העלאת חלקי מידע לצורך גיבוי, מתחייב הספק לפנות לקבלת אישור מנהל תחום אבטחת המידע והסייבר בנתיבי איילון וכן לנקוט באמצעי הגנה נאותים על מנת להבטיח את שלמות, סודיות וזמינות המידע.
3. במידה ונדרש מהספק לצורך פעילותו לבצע העלאת חלקי מידע לקלטת גיבוי מתחייב הספק לוודא כי אין עירוב של מידע מסיווגים שונים על אותו התקן.
4. במאגר מידע שניתן להתחבר אליו מרחוק באמצעות רשת האינטרנט למטרות ניהול, הספק מתחייב לבצע הזדהות חזקה ורב שלבית (MFA).

ט. גיבוי ושחזור מידע

1. מידע של נתיבי איילון הנמצא במערכות הספק יגובה באופן סדיר וזאת על-פי מדיניות שתתווה נתיבי איילון.
2. הספק מתחייב לבצע גיבויים מאובטחים של המידע הנצבר אצלו.
3. הספק מתחייב לאחסן את מדיות הגיבוי באופן מאובטח.
4. במידה ויש שימוש בספקי צד שלישי לאחסון גיבויים, יש לאשר זאת טרם תחילת העבודה אל מול נתיבי איילון.
5. הספק מתחייב לבצע שחזורים מדגמיים של המדיות המגבות על תשתיותיו לצורך בדיקות שחזור התאוששות.
6. לאחר סיום השחזור המדגמי מתחייב הספק למחוק את המידע ששוחזר.
7. הספק מתחייב כי שחזור יבוצע אך ורק באישור ממונה אבטחת המידע והסייבר של נתיבי איילון.
8. הספק מתחייב כי במידה ובוצע שחזור יתועדו כל הליכי השחזור כולל זהותו של מבצע השחזור.
9. הספק מתחייב למנוע עירוב מידע מסיווגים שונים בזמן השחזור.
10. הספק יערך לרציפות תפקודית ולהתמודדות עם מצבי משבר בסייבר בהתאם לתרחישי האיום שיוגדרו ויעודכנו מעת לעת על-ידי מערך הסייבר הלאומי, משרד התחבורה ונתיבי איילון.

11. ההיערכות תכלול לכל הפחות גיבוש מדיניות ונהלי תגובה לאירועי סייבר, הגדרת תפקידים אחריות, הכנת תשתיות חלופיות, גיבוי המידע והגדרת חלופות לתהליכים מרכזיים.

י. פיתוח תוכנה

1. בכל הנוגע לפיתוח תכנה על הספק לעמוד [בדרישות פיתוח מאובטח](#) (SSDLC) של מערך הסייבר הלאומי.
2. קוד התוכנה יכיל רק את הנרשם בתיעוד המסופק עם התוכנה ואשר סוכם עם נתיבי איילון.
3. קוד התוכנה יהיה ללא רישום סיסמאות ניהול, דלתות אחוריות וכיו"ב.
4. התוכנה תיבדק ע"י בודקי חדירות, בלתי תלויים, בתהליך Code Review בצורה מעמיקה, כולל תיקון באגים הפוגעים באבטחת המידע של המערכת. פגיעות זו, במידה וקיימת תתוקן ודיווח על כך יועבר לנתיבי איילון.
5. המערכת לא תבצע שינויי קוד במערכות נלוות כגון מערכת הפעלה, אשר פוגעים ברמת אבטחת המידע הכללית של מערכות המחשוב של המזמין.
6. הספק מתחייב כי בגרסאות עתידיות של המערכת לא יתבצעו שינויים מהותיים ללא אישור נתיבי איילון.
7. התשתיות והפלטפורמות יותקנו ע"י הספק תוך שימוש בתוכנות ורישיונות מקור בלבד. בשימוש בתוכנות יש לוודא בדיקת הלבנה לפני ההתקנה למניעת החדרת קוד עוין. בשימוש במערכות וירטואליות יש להתקין מחדש קובץ MASTER מהימן ובדוק.
8. בדיקת פיתוח קוד בהיבט אבטחת מידע - על הספק לפתח קוד בהתאם לדרישות אבטחת המידע המפורטות לעיל. המשרד יהיה רשאי לעשות בדיקות ברמת הקוד כדי לוודא כי דרישות אלה מולאו.

יא. ביקורת חצרות ספק

1. הספק מתחייב לבצע מדי שנה סקר אבטחת מידע ומבדק חדירה לרשת התקשורת שלו ולמערכותיו באמצעות צד שלישי שזהותו אושרה על ידי המזמין, ולהעביר [תקציר מנהלים שלאת ממצאי](#) הסקר ומבדק החדירה לעיונו של מנהל אבטחת המידע של נתיבי איילון.
2. נתיבי איילון או מי מטעמה רשאים לערוך ביקורות (באמצעות מחלקת אבטחת מידע של המזמין ו/או ע"י ספק חיצוני המועסק מטעמו) בחצרות או במערכות הספק (מעבר לאלה שתערוך חברת אבטחת המידע בה יבחר הספק) לשם ווידוא עמידה בהנחיות מסמך זה ו/או לצורך זיהוי כל סיכון אפשרי על המידע של המזמין. ביקורות אלו עשויות לכלול, על פי שיקול דעתו של המזמין, את אלה:

- בקרה על תהליכי ונהלי עבודה רלוונטיים לעבודת הספק מול המזמין.
- יישום אמצעי אבטחת המשאב האנושי בחצרות הספק.
- יישום אמצעי אבטחה פיסית וסביבתית בחצרות הספק; יישום אמצעי אבטחה לוגית בחצרות הספק (כולל כניסה למערכות הספק ו/או בדיקה באמצעות כלים ממוכנים ברשת ומערכות הספק)
- בחינת חוסן מערכות המידע של הספק מתוך או מחוץ לרשת הספק על ידי גורם חיצוני בלתי תלוי, כפי שיוגדר על ידי המזמין (תוך תיאום עם הספק ובהסכמתו).

1. נתיבי איילון תדרוש מהספק את מחיקת המידע בסיום ההתקשרות, או בכל נקודת זמן שקודמת לה (לדוגמה במקרה של חשד לפריצה ו/או דלף מידע אצל הספק).
 2. יש לוודא כי הסדרים עם הספק שנקבעו במסגרת הסכם ההתקשרות, מתקיימים. בפרט חשוב לוודא עמידה בכל הקשור למחיקת נתונים של נתיבי איילון המאוחסנים בחצרי הספק בתום ההתקשרות בין הצדדים. בין היתר יש לבדוק את הנושאים הבאים:
 - יש לוודא החזרת כלל הרשומות, המדיה, הציוד והרכיבים השייכים לארגון אשר נעשה בהם שימוש לצורך עבודת הספק. כל זאת, לרבות פריטים הנמצאים בקרב כלל עובדי הספק וספקי המשנה שלו.
 - הספק יחתום על הצהרה בה הוא מתחייב שלא נשארו ברשותו רכיבים כלשהם הנוגעים למערכת ו/או מידע אודות נתיבי איילון וכי הוא לא יעשה שום שימוש במידע על נתיבי איילון, אליו הוא נחשף במסגרת ההתקשרות.
 - יש לוודא השמדת מדיה מגנטית מכל ציוד אשר שימש את הספק במהלך ההתקשרות עם נתיבי איילון (כגון: במקרה שמדובר במחשבים של הספק ששימשו לעיבוד ו/אחסון של מידע של נתיבי איילון).
 - נדרש לוודא מחיקת עותקים של קבצים ומידע של נתיבי איילון ממערכות המידע ונכסי ה-IT של הספק לאחר סיום הצורך העסקי באחזקתו.
- ❖ אי יישום העקרונות המובאים במסמך זה בחלקם או במלואם עלול להביא להפסקת ההתקשרות בהתאם לשיקול דעתה המקצועי של נתיבי איילון או מי מטעמה.