

נתיבי איילון - דרישות אבטחת מידע למפעילים

עבור מכרז נעים לירוק

תוכן עניינים

1.....	תוכן עניינים
2.....	כללי
2.....	רגולציה ומשפט
2.....	עמידה בתקני אבטחת מידע
2.....	ארכיטקטורה וגבולות
3.....	אישור עובדים
3.....	פיתוח מאובטח
3.....	שימוש ברכיבי אבטחת מידע
3.....	אבטחת מידע בתנועה
4.....	תקשורת
4.....	אבטחת נתונים נייחים
4.....	אחסון וגיבוי
4.....	בקרת גישה
4.....	הזדהות:
4.....	סיסמאות:
5.....	התחברות וניתוק:
5.....	ניהול הרשאות וזהויות
5.....	אבטחת היישום הסלולרי (ככל שיסופק יישום כזה ע"י המפעיל)
5.....	נגישות למידע על-ידי אנשי המפעיל
5.....	מעקב ובקרה
6.....	ביקורת
6.....	מניעת Lockdown
6.....	סיום התקשרות עם מפעיל

כללי

מסמך זה מציג את דרישות אבטחת מידע למפעילי ניסוי "נעים לירוק". הניסוח מופנה למפעיל בודד, כאשר ההוראות ישימות לכל מפעל שייבחר לספק את השירות במסגרת מכרז זה.

יובהר, כי על המפעיל לעמוד בכל דרישות אבטחת המידע המפורטות בהסכם ההתקשרות, בכתב ההתחייבות לעניין הגנת הפרטיות המצורף כמסמך ד' למסמכי המכרז, ובמסמך זה. בכל מקרה של סתירה ו/או אי התאמה ו/או דו משמעות ו/או חוסר בהירות הקיימת לדעת המפעיל בין הוראה אחת מהוראות מסמך זה לבין הוראה אחרת בהסכם ההתקשרות ו/או במסמך ד' להסכם, או שהיה המפעיל מסופק בפירושם הנכון של הוראה, מסמך או כל חלק מהם - יפנה המפעיל לחברה, קודם לחתימת ההסכם או באופן מיידי לאחר הגילוי כאמור, והחברה תיתן הבהרות ו/או הוראות בכתב, בדבר הפירוש שיש לנהוג לפיו. הכרעת החברה באשר לסתירה ו/או אי התאמה ו/או חוסר בהירות כאמור לעיל, נתונה לשיקול דעתה הבלעדי של החברה ומחייבת את המפעיל לכל דבר ועניין.

מבלי לגרוע מכלליות האמור לעיל, בכל מקרה של סתירה ו/או אי התאמה בין המסמכים השונים, תגברנה ההוראות המחמירות יותר עם המפעיל, בהתאם לשיקול דעת החברה בעניין.

רגולציה ומשפט

כל מפעיל ימנה ממונה הגנת סייבר ואבטחת מידע – מצוות אבטחת המידע של המפעיל ובעל הכשרה מתאימה שאחראי על הגנת סייבר ואבטחת המידע הנכלל במאגרי המידע של החברה המאוחסנים במערכות ובשרתי המפעיל כנדרש בחוק הגנת הפרטיות התשמ"א 1981 ותקנות אבטחת המידע.

ממונה אבטחת המידע יהיה אחראי על יישום ההנחיות של תחום סייבר בנושאי הגנת סייבר ואבטחת מידע.

ממונה אבטחת המידע של המפעיל יעמוד בקשר שוטף עם תחום אבטחת המידע אצל המזמינה.

עמידה בתקני אבטחת מידע

על המפעיל לעמוד בתקני אבטחת מידע הבאים:

- תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז - 2017, בכל הנוגע לניהול מאגרי מידע הכוללים מידע אישי.
- ככל שהמפעיל יבסס את המערכות המרכזיות על שירותי ענן, המסופקים ע"י קבלן משנה, על קבלן לעמוד בתקן 270001. יועדפו מפעילים התומכים CSA STAR.

ארכיטקטורה וגבולות

המפעיל יהיה אחראי לתכנון מערך אבטחת המידע שיופעל במסגרת המערכות המסופקות. התכנון יכלול את כלל הכלים והנהלים שיוספקו ויושמו במערכות, לצורך עמידה ברמת אבטחת המידע הנדרשת במסגרת מסמך זה. תכנון זה יאושר ע"י צוות אבטחת המידע מטעם החברה.

בנוסף, יהיה המפעיל אחראי להכנת נהלי אבטחת מידע, אשר יגדירו, בין השאר, את גבולות הגזרה ותחום האחריות של המפעיל ושל החברה.

אישור עובדים

לכלל העובדים, אשר יהיו נגישים למידע של החברה ושל המתנדבים, תבוצע בדיקת רישום פלילי ומבדק אמינות ממוחשב. רק עובדים שיאושר בסיום תהליך זה יורשו לפעול במערכת.

החברה תהא רשאית לדרוש החלפת כל עובד, שלגביו יתעורר חשש כי איננו עומד בתנאים ובסטנדרטים, עליהם מחויבת החברה.

פיתוח מאובטח

המפעיל ייקבע נהלים שיבטיחו כי כל הפיתוח שיבוצע יישמר את רמת אבטחת המידע הנדרשת. הנהלים יכללו, לכל הפחות:

1. הכנת נוהל פיתוח קוד מאובטח, שיחייב את כל צוות הפיתוח. דוגמא לנוהל דומה ניתן למצוא בנהל משרד הבריאות לפיתוח מערכות מאובטחות בכתובת https://www.health.gov.il/services/tenders/doclib/mi16_2013r.pdf.
2. מינוי מומחה לפיתוח מאובטח, שיהיה אחרא להטמעת מימוש הנוהל הנ"ל בתהליכי הפיתוח.
3. ביצוע הדרכות לכל צוותי האפיון, הפיתוח והבדיקות, לכל הנדרש למימוש הנוהל.
4. שימוש כלי ממוכן, כדוגמת Checkmarx, לבדיקת כל קוד, לפני הפעלתו במערכת.

שימוש ברכיבי אבטחת מידע

המפעיל יעשה שימוש ברכיבי אבטחת המידע הבאים, לכל הפחות:

1. התקני firewall, שימשו לחציצה בין רשתות בסיווגים שונים, להגנת הממשקים למזמינה ולמפעיל המערכות המרכזיות, לחיבור לרשת ה-Internet וגורמים חיצוניים ולחציצה בין משתמשים ושרתים.
2. התקני WAF, להגנת אתרי WEB.
3. XML firewall, להגנת הממשקים מול המזמינה ומול מפעיל המערכות המרכזיות.
4. התקני IPS, להגנת הקישור לרשת ה-Internet.
5. התקני DLP, למניעת הוצאת מידע שאיננו מאובטח אל מחוץ לרשת.
6. תוכנות אנטי-וירוס, לכלל העמדות והשרתים ברשת.
7. מערכת NAC, למניעת גישה בלתי מורשת לרשתות המפעיל.
8. מערכת SIEM, לאיסוף, ניטור וניתוח אירועי אבטחת מידע.

אבטחת מידע בתנועה

המפעיל נדרש להעביר מידע אשר נמצא בתנועה כגון מידע העובר בין המערכות המרכזיות למערכות המפעיל, ובין מערכות המפעיל ליישום הסלולרי, על גבי תווך תקשורת מוצפן לפחות אחד מאלה: (SSL/IPSEC/VPN/SSH וכו').

המפעיל יידרש לאבטח את המערכות על ידי אמצעים להגנה מפני מתקפות מסוג DDOS תשתית ואפליקטיבי.

המפעיל יספק פתרון אבטחה מתקדם המספק 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.

תקשורת

המפעיל יתמוך בקישור למערכות המרכזיות בשתי החלופות הבאות:

1. דרך האינטרנט בתוך מוצפן. קישור זה יוגבל לכתובות ה-IP של החברה.
2. באמצעות תשתית ייעודית מוצפנת בין המפעיל לחברה אשר תאפשר רציפות עבודה במידה והגישה למפעיל דרך רשת האינטרנט לא תתאפשר.

אבטחת נתונים נייחים

ככל שיבחר המפעיל להפעיל את מערכתיו על גבי תשתית ענן ציבורי, המפעיל יצפין מידע רגיש תוך שימוש באלגוריתם הצפנה סטנדרטי ומוכר. מידע רגיש הינו מידע המוגדר כרגיש על פי חוק הגנת הפרטיות התשמ"א 1981 או שהוגדר כך על-ידי החברה.

לצורך מימוש ההצפנה יעשה שימוש במערכת HSM, שתאפשר לחברה לשמור את מפתחות הצפנה אשר יהיו בשליטה בלעדית של החברה (חילול והחלפת מפתחות, למפעיל לא תהיה גישה למערכת ה-HSM, למעט לצורכי הצפנת מידע).

על המפעיל להציג בפני החברה את ארכיטקטורת אחסון הנתונים כדי לאפשר לחברה לזהות סיכונים אבטחתיים ובקורות זמינות להתמודדות עם סיכונים אלו.

אחסון וגיבוי

המידע המנוהל במערכות לא ייצא מתחומי המדינות המופיעות המותרות לאחסון נתונים אישיים, על פי הנחיות הרשות להגנת הפרטיות במשרד המשפטים. אתר הגיבוי של המפעיל יהיה כפוף לאותה הרשימה.

המערכות תגובנה בתדירות שלא תפחת מאחת ליום, כאשר הגיבויים יישמרו מחוץ לאתרי המחשוב.

בקרת גישה

הזדהות:

על המפעיל לתמוך בלפחות שניים מאמצעי ההזדהות הבאים:

- Something you know: סיסמה מורכבת, בעת אורך מינימלי.
- Something you have: כרטיס חכם (Smart Card), RSA Token, קוד OTP (One Time Password) הנשלח באמצעות SMS או מופק דרך טלפון/התקן חכם אחר.
- Something you are: אמצעי ביומטרי כגון טביעת אצבע, רשתית עין וכדומה.

סיסמאות:

במידה ונעשה שימוש בסיסמאות, המפעיל יידרש לעמוד במדיניות הסיסמאות הבאה:

- מורכבות סיסמה: תהיה מורכבת מ-8 תווים או יותר הכוללים אותיות קטנות וגדולות, ספרות וסימנים מיוחדים.

- תוקף סיסמה: תוקף הסיסמה יפוג לאחר תקופה של עד 90 יום ולאחר מכן יידרש המשתמש להחליפה.
- היסטוריית סיסמאות: תשמר היסטוריית סיסמאות של לפחות 10 סיסמאות לאחור.

התחברות וניתוק:

ניסיונות הזדהות שגויים באמצעות כל אחד משלושת שיטות ההזדהות שהוזכרו תוביל לנעילת המשתמש למשך 15 דקות.

יגדר פרק זמן קבוע שלאחריו יופעל מנגנון ניתוק תקשורת (session time out) המחייב זיהוי מחדש של המשתמש.

ניהול הרשאות וזהויות

יש להגדיר הרשאות גישה למידע באופן מדוקדק תוך הענקת הרשאות גישה רק לגורמים אשר גישתם למידע הכרחית לצורך מילוי תפקידם.

אבטחת היישום הסלולרי (ככל שיסופק יישום כזה ע"י המפעיל)

היישום הסלולרי יפותח בהתאם לעקרונות הבאים:

1. כל המידע האישי, המנוהל על גבי המכשיר הסלולרי, יוחזק בצורה מקודדת, שלא תאפשר גישה ישירה לנתונים, שלא באמצעות האפליקציה.
2. לצורך הפעלת היישום, יהיה על המתנדב להירשם לשירות על גבי המכשיר הספציפי, בו הינו עושה שימוש. היישום יכלול אמצעים שימנעו העתקתו למכשיר סלולרי אחר, ללא רישום מחדש של המכשיר.
3. כניסה לנתונים האישיים של המתנדב, לרבות נתוני ייתרה והיסטורית נסיעות, תחייב הזדהות באמצעות pin code של 6 ספרות לפחות, או באמצעות טביעת אצבע.

נגישות למידע על-ידי אנשי המפעיל

יש לצמצם את קבוצת אנשי המפעיל היכולים לשלוף את כלל המידע למינימום.

כל פעולות ה-DBA ינטרו ברמה פרטנית ובאופן חד ערכי וכל פעילות של יצירה שינוי בבסיסי הנתונים ובמידע תועבר לצוות אבטחת המידע.

מידע של מתנדבים לא יוצא החוצה שלא בדרך שסוכמה עם החברה.

מעקב ובקרה

רישומי המערכת ייאספו ע"י מערכת SIEM או Syslog ייעודית או ישלחו למערכת ה-SIEM של החברה לצורך ניטור והתראה על אירועי אבטחה המתרחשים במערכות.

על מפעיל השירות לאפשר לחברה, או מי מטעמו לאסוף את רישומי המערכת בזמן אמת/באופן מתוזמן.

הלוגים יועברו בפורמט UTC.

המפעיל מתחייב לשמור לאחור רישומי מערכת לתקופה המשתנה בהתאם לרגישות המערכת ולדרישות רגולטוריות התקפות למערכת.

על המפעיל לוודא כי רישומי המערכת נשמרים בשרת מרכזי המנוהל ע"י צוות עובדים נפרד.

במקרה בו ישנה המפעיל את מערכת הלוגים עליו לעדכן את החברה 60 יום מראש על מנת שתוכל להיערך.

המפעיל יידרש לבצע ניטור לשירותים ומערכות ברבדים הבאים:

- ניטור לוגים - איתור בזמן אמת או בדיעבד של בעיות טכניות או אירועי אבטחת מידע המתרחשים.
- ניטור ביצועים – מעקב אחר עומסים במשאבי המחשוב.
- ניטור ומעקב אחר פעילויות חריגות/עויינות (ניסיונות הזדהות כושלים, גישה לא מורשית, ניסיונות כניסה כפולים ועוד).

אירועים שיוגדרו ברמת סיכון גבוה כגון חשד לנגישות זרה ו/או הזלגת מידע ממאגר הנתונים המפעיל יעדכן באופן מיידי את החברה (על פי רשימת תיוג מוגדרת) ויודיע את אופן הטיפול בהם.

ביקורת

אחת ל-18 חודשים, לכל הפחות, יבצע המפעיל:

- מבדקי חדירה. מבדקים אלו יבוצעו ע"י חברה מתמחה ייעודית, שלא הייתה מעורבת בתהליך הקמת המערכות.
- סקר סיכונים כולל.

תוצאות הסקרים והמבדקים יוצגו לחברה בפגישה שנתית. על המפעיל להציג תכנית לתיקון הממצאים במידה ויש. במקרה של ליקויים מהותיים המשפיעים ישירות על מערכות החברה יש לידע באופן מיידי את החברה על המצאות הליקוי.

המפעיל יאפשר לנציגים מטעם החברה לקיים סיור במתקניו הרלוונטיים לשם ביקורת אבטחת מידע ועמידה בהסכמים ו/או חוזים אשר נחתמו מול החברה.

מניעת Lockdown

המפעיל יאפשר לחברה לשמור עותק מקומי של כל מידע בחצרות החברה ו/או בכל אתר אחר של החברה.

סיום התקשרות עם מפעיל

עם סיום ההתקשרות עם הספק, על המפעיל מוטלת האחריות לבצע את הפעולות הבאות:

- מחיקה חד חד ערכית ולא ניתנת לשחזור של כל הנתונים והמידע השמורים במערכות.
- השמדת עותקים של הנתונים והמידע בהם נעשה שימוש במסגרת פעילות המפעיל עבור החברה.

- דרישה מהמפעיל להציג הוכחות לכך שהמידע הושמד (רישומים ודוחות רלוונטיים).
- במידה והמידע הוצפן – ביטול (Revoke) מפתחות ההצפנה ומחיקתם.