

מכרז ממוכן (מקוון) מס' 23/20 למתן שירותי תחזוקה עדכון ופיתוח מערכת מידע לתחבורה ציבורית עבור חברת נתיבי איילון – נספח אבטחת מידע

1. מטרה
- 1.1 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 ומערכות המידע השייכים לנתיבי איילון.
- 1.2 כל הדרישות במסמך מופנות לספק אך יחולו על כל מי שמעורב במתן השירותים מטעמו, אלא אם נרשם מפורשות אחרת..

2. הגדרות

- 2.1 נציג הביטחון – נציג מטעם נתיבי איילון / החברה לעניין ביטחון המידע .
- 2.2 הספק – כולל עובדיו, נציגיו, קבלני משנה ונותני שירות מטעמו.

3. נאמן אבטחת מידע

- 3.1 הספק ימנה נאמן הגנת סייבר ואבטחת מידע – מצוות אבטחת המידע של הספק ובעל הכשרה מתאימה שיהיה אחראי על הגנת סייבר ואבטחת המידע הנכלל במאגרי המידע של המזמין המאוחסנים במערכות ובשרתי הספק כנדרש בחוק הגנת הפרטיות, התשמ"א-1981 ותקנות אבטחת המידע.
- 3.2 נאמן אבטחת המידע ישמש כאיש הקשר בין הספק לגורמי הביטחון של נתיבי איילון.

4. מהימנות צוות הספק

- 4.1 כל נציג בצוות הספק שייקח חלק בפרויקט ייבדק בדיקת מהימנות על ידי נציג הביטחון, כאשר בדיקה זו מהווה תנאי לתחילת העבודה של כל נציג. הדרישות יהיו תקפות לגבי קבלני משנה, עובדים ארעיים וכל נותן שירותים אחר מטעם הספק.
- 4.2 הספק מתחייב כי
- 4.2.1 יעסיק בכל העבודות הקשורות בביצוע המכרז אך ורק עובדים שאושרו להעסקה על ידי נציג הביטחון.
- 4.2.2 לא יעסיק במתן השירותים הנדרשים עובדים מטעמו שטרם אושרו, לא יחשוף בפניהם כל חומר הקשור לביצוע הסכם זה בטרם קבלת האישור כאמור.

- 4.2.3 לא יחשוף בפני אלה כל חומר הקשור לביצוע הסכם זה בטרם סיימו את תהליך מהימנות העובדים והורשו בידי נציג הביטחון לספק שירותים לנתיבי איילון.
- 4.2.4 לא יאפשר גישה לאתרים בהם יעבוד, לגורמים שאינם מוסמכים לכך
- 4.3 באחריות נאמן אבטחת המידע מטעם הספק לוודא את מילוי הטפסים בעבור כלל העובדים שייקחו חלק בפרויקט מטעמו לרבות קבלני משנה, ולהעבירם לנציג הביטחון ולבצע מעקב על אישור הנציגים המאושרים לעבודה.
- 4.4 נאמן אבטחת המידע יעדכן באופן שוטף את נציג הביטחון בכל שינוי במצבת העובדים בפרויקט.
- 4.5 הספק מתחייב לעדכן באופן מידי את נציג הביטחון על כל עובד, שהעניק שירותים למזמין, המפסיק את עבודתו בחברה עם קבלת הידיעה על העזיבה וסיבת העזיבה.
- 4.6 נציג הביטחון שומר לעצמו את הזכות לפסול כל אחד מהעובדים ללא צורך בנימוק או הסבר כלשהו והחלטתו תהיה סופית ומכרעת.
- 4.7 הספק יתחייב לעמוד בלוח הזמנים לביצוע חלקו בפרויקט, ללא תלות באישור ביטחוני לעובדים מסוימים, או בהרחקת עובדים, לפני או במהלך העבודה, ובתנאי שאישור/ סירוב יינתן ע"י נציג הביטחון תוך 10 ימי עבודה, ממועד קבלת המסמכים הרלוונטיים מהספק.

5. סודיות

- 5.1 הספק מצהיר בזאת שידוע לו כי המידע שיתקבל במהלך מתן השירותים אליו או למי מטעמו הוא בעל רגישות מיוחדת, והוא מתחייב כי הוא או מי מטעמו לא יעבירו מידע זה לכל גורם אחר שבו או עימו הוא קשור שלא לצורך מתן השירותים, אלא אם כן ניתן לכך אישורו המוקדם של נציג הביטחון ובתנאים כפי שייקבעו על ידו.
- 5.2 הספק מצהיר, כי הוא מכיר את הוראות חוק הגנת הפרטיות, התשמ"א-1981, והתקנות שהותקנו על פיו, וכי יפעל כמתחייב מחוק זה ומכל חיקוק אחר הנוגע לשמירתו וסודיותו של המידע שימצא ברשותו.
- 5.3 נציג הביטחון רשאי למסור הנחיות נוספות בנושא שמירה על סודיות ואבטחת מידע במהלך תקופת ההתקשרות בכתב או בעל פה, ואלה יחייבו את הספק ללא יכולת ערעור מצד הספק.
- 5.4 אם תחול על הספק או מי מטעמו חובה על פי דין לגלות מידע שהוא חייב שמירתו בסוד לפי ההסכם, הוא יודיע על כך לנציג הביטחון מראש ובאופן מיידי.

6. עמידה בתקני אבטחת מידע

- 6.1 מתקני אחסון המידע של ספק שירותי הענן מטעם הספק נדרשים לעמוד בתקני אבטחת המידע הייעודיים/מותאמים לסביבות ענן:
- 6.1.1 ISO/IEC 27017
 - 6.1.2 ISO/IEC 27018:2014
 - 6.1.3 ISO/IEC 27036-x
 - 6.1.4 AICPA SOC 2/3
 - 6.1.5 ISO/IEC 27001/27002
 - 6.1.6 ISO 27032

PCI DSS 6.1.7

COBIT 6.1.8

7. אבטחת מידע

- 7.1 הספק יבצע סריקות אנטי וירוס על רשת הספק בלבד ולא על מידע של המזמין.
- 7.2 הספק יספק מערכת בקורות למזמין המאפשרת למזמין לבצע ניטור מהיכן בוצע חיבור למערכת.
- 7.3 הספק יערוך מבדקי חדירה וסקרי סיכונים לפחות אחת לשנה. תוצאות הסקרים והמבדקים יוצגו לנציג הביטחון אחת לשנה.
- 7.4 על הספק להציג תכונות לתיקון הממצאים במידה ויש. במקרה של ליקויים מהותיים המשפיעים ישירות על מערכות נתיבי איילון יש לידע באופן מידי.

8. אירועי אבטחת מידע

- 8.1 על הספק ומי מטעמו לדווח על כל ליקוי אבטחת-מידע, שיגלה ישירות לנציג הביטחון. הדיווח יכלול כל אירוע של הפרה או חשש להפרת הוראות ביטחון לרבות:
 - 8.1.1 בכל מקרה של תקלת אבטחה באתר המזמין או באתר הספק, במקרים הרלוונטיים לביצוע העבודה.
 - 8.1.2 בכל אירוע בו מעורב גורם-חוץ או אחד מעובדיו, או שקיים חשד למעורבות שיש עמה השלכה ישירה או עקיפה על ביטחון המזמין.
 - 8.1.3 בכל הפרה או חשד להפרה של חוקים, תקנות או נוהלי אבטחת-מידע.
- 8.2 הספק מתחייב לנהל דו"חות ומעקב איתור אירועים חריגים, דיווח וטיפול בהם.
- 8.3 הספק ינהל יומן אירועי ביטחון ויצגם לנציג הביטחון, בהתאם לדרישה.
- 8.4 נציג הביטחון ראשי להגדיר מהו אירוע או ליקוי מהותי, אופן הדיווח, הגורמים המדווחים והנמענים לדיווח.
- 8.5 בסמכות נציג הביטחון לעדכן את הנחיות אבטחת המידע בעקבות אירוע אבטחת מידע. על הספק לציית לדרישות.

9. בקרה ופיקוח

- 9.1 בסמכות נציג הביטחון ונציג שיוסמך על ידו לבצע סיקרי-סיכונים, ביקורות פתע, בדיקות ביטחוניות, בדיקות חסינות, ביקורות הדרכה וכל ביקורת אחרת באתר הספק, אשר מטרתה לבחון תקינות מערכי אבטחה, סיכונים, יעילות פתרונות אבטחה או בדיקת חשדות, אשר להם זיקה או השפעה על אבטחת המערכות המשמשות את המזמין.
- 9.2 הספק יאפשר למזמין או למי שימונה מטעמו לפקח על אספקת השירותים המבוקשים, טיבם ואיכותם, ולהיכנס לצורך זה לכל מקום, על מנת לבדוק ולפקח על אופן מילוי התחייבויותיו.
- 9.3 הספק מתחייב לשתף פעולה עם נציגי המזמין או מי מטעמו, בכל הנוגע להוראות הביטחון הנוגעות לפרויקט וימלא אחר כל הנחיה של נציגי המזמין בכפוף להוראות המכרז וההסכם. בכלל זה, ימסור לנציג המזמין כל מידע או דיווח שיידרש על ידיהם, במועד ובאופן שייקבע על ידיהם; יאפשר לנציגי המזמין לבקר במשרדיו ובכל מקום אחר שבו הוא מבצע את התחייבויותיו על פי הסכם זה, לעיין בכל מסמך ולבדוק את הנעשה בהם בקשר לשירותים

ולביצוע התחייבויות הספק על פי הסכם זה, ובלבד שכל ביקור כאמור יתואם מראש עם הספק.

10. תקשורת

- 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 נדרש להעביר מידע אשר נמצא בתנועה כגון מידע העובר בין נתיבי איילון לענן, בין ספקי ענן שונים או בין רכיבים שונים בתוך הענן, על-גבי תווך תקשורת מוצפן לפחות אחד מאלה: (SSL/IPSEC/VPN/SSH וכו').
- 10.5 הספק יידרש לאבטח את המערכות על-ידי אמצעים להגנה מפני מתקפות מסוג DDOS תשתית ואפליקטיבי.
- 10.6 הספק 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.

11. אבטחת נתונים נייחים

- 11.1 הספק מתחייב לאחסן את נתוני המידע של נתיבי איילון בשיטה כגון IDA, מנגנון המאפשר לפצל את המידע המאוחסן בשרתי הספק בין מספר שרתי אחסון שונים במטרה להקשות על תוקף בהשגת המידע בשלמותו.
- 11.2 הספק יאפשר למזמין להצפין מידע רגיש השמור בענן 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 נציג הביטחון.
- 11.3 הספק יאפשר למזמין להתמים (MASKING) מידע בענן על-פי שיקול דעת המזמין.
- 11.4 הספק יתמוך באפשרות ששדה מהותי אחד לפחות (שדה מזהה המאפשר זיהוי חד ערכי) יאוכסן ברשת המזמין.
- 11.5 על הספק וספק להציג בפני נתיבי איילון את ארכיטקטורת אחסון הנתונים כדי לאפשר לנתיבי איילון לזהות סיכוני אבטחה ובקורות זמינות להתמודדות עם סיכונים אלו.

12. הזדהות

- 12.1 בעת טעינת נתוני נתיבי איילון למערכות הענן על הספק לתמוך בלפחות שניים מאמצעי ההזדהות הבאים:
 - 12.1.1 Something you know: סיסמה מורכבת וארוכה MFA.
 - 12.1.2 Something you have: כרטיס חכם (Smart Card), RSA Token, קוד OTP (One Time Password) הנשלח באמצעות SMS או מופק דרך טלפון/התקן חכם אחר.

- 12.1.3 Something you are: אמצעי ביומטרי כגון טביעת אצבע, רשתית עין וכדומה.
- 12.2 במידה ונעשה שימוש בסיסמאות, יש לאשר מראש את השימוש. הספק יידרש הספק לעמוד במדיניות הסיסמאות הבאה:
- 12.2.1 מורכבות סיסמה: תהיה מורכבת מ-12 תווים או יותר הכוללים אותיות קטנות וגדולות, ספרות וסימנים מיוחדים.
- 12.2.2 תוקף סיסמה: תוקף הסיסמה יפוג לאחר תקופה של עד 90 יום ולאחר מכן יידרש המשתמש להחליפה.
- 12.2.3 היסטוריית סיסמאות: תשמר היסטוריית סיסמאות של לפחות 10 סיסמאות לאחור.
- 12.2.4 ניסיונות הזדהות שגויים באמצעות כל אחד משלושת שיטות ההזדהות שהוזכרו תוביל לנעילת המשתמש למשך 15 דקות.
- 12.3 יוגדר פרק זמן קבוע שלאחריו יופעל מנגנון ניתוק תקשורת (session time out) המחייב זיהוי מחדש של המשתמש.
- 12.4 ניהול הרשאות וזהויות לסביבת הניהול של נתוני נתיבי איילון - הספק נדרש לנהל את הגישה לשירותי הענן לפי סוג ההתקן (מחשבים ניידים/ניידים, טלפונים חכמים וכו'), מיקום וכתובות. יש להגדיר הרשאות גישה למידע באופן מדוקדק תוך הענקת הרשאות גישה רק לגורמים אשר גישתם למידע הכרחית לצורך מילוי תפקידם לדוגמא IAM . הרשאות הגישה לשירותי הענן ינוהלו על-ידי נתיבי איילון.
- 12.5 הספק יאפשר שימוש במערכת ה-IDM של נתיבי איילון או במערכת SCIM לניהול זהויות והרשאות משתמשים. החיבור לנתיבי איילון יבוצע על-ידי פרוטוקולים סטנדרטיים.

13. ניהול מפתחות הצפנה

- 13.1 הספק יאפשר לנתיבי איילון לנהל את מפתחות ההצפנה באופן עצמאי בשטח הארגון או על-ידי גורם צד שלישי המתמחה בניהול מפתחות הצפנה.
- 13.2 במידה ויקבע הלקוח (נתיבי איילון) שברצונו לנהל את מפתחות ההצפנה בענן, על ספק השירות לספק רכיב ייעודי לאחסון וניהול מפתחות הצפנה באופן מאובטח בהתאם לדרישות נתיבי איילון.
- 13.3 הספק יעמוד בתקני אבטחה מחמירים כגון FIPS 14-2, Common Criteria EAL4+ וכדומה, ויתמוך בפרוטוקולי הצפנה סטנדרטים ומוכרים.

14. מעקב ובקרה

- 14.1 ספק השירות יידרש לספק דוחות כגון SSAE 16 SOC2 או ISAE 3402 Type 2 report אודות בקרות הנעשות בשטחו על-ידי גופים חיצוניים אמינים הסוקרים נושאים הקשורים לאבטחת המידע, זמינותו, שלמותו וחשאיותו, וכן בקרות הקשורות להגנה על הפרטיות.
- 14.2 בהתאם למודל השירות הנבחר ולסוג המערכת/מידע הנשמרים בענן, על ספק השירות להבטיח את אמינות נתוני הרישום של אירועים במערכות/רכיבים שהוגדרו על-ידי נתיבי איילון כבעלי רגישות גבוהה לתפקוד המערכת.
- 14.3 רישומי המערכת ייאספו על-ידי מערכת SIEM או Syslog ייעודית בענן או ישלחו למערכת ה-SIEM של נתיבי איילון או מערכת אחרת בהחלטת נתיבי איילון לצורך ניטור והתראה על אירועי אבטחה המתרחשים בענן.

- 14.4 על ספק לאפשר לנתיבי איילון או מי מטעמו לאסוף את רישומי המערכת בזמן אמת/באופן מתוזמן.
- 14.5 הלוגים יועברו בפורמט UTC.
- 14.6 הספק מתחייב לשמור לאחור רישומי מערכת לתקופה המשתנה בהתאם לרגישות המערכת ולדרישות רגולטוריות התקפות למערכת.
- 14.7 על הספק לוודא כי רישומי המערכת נשמרים בשרת מרכזי המנוהל על-ידי צוות עובדים נפרד.
- 14.8 במקרה בו ישנה הספק את מערכת הלוגים עליו לעדכן את המזמין 60 יום מראש על מנת שיוכל להיערך. הספק יידרש לבצע ניטור לשירותים ומערכות בענן ברבדים הבאים:
- 14.8.1 ניטור לוגים – איתור בזמן אמת או בדיעבד של בעיות טכניות או אירועי אבטחת מידע המתרחשים.
- 14.8.2 ניטור ביצועים – מעקב אחר עומסים במשאבי המחשוב בענן.
- 14.8.3 ניטור ומעקב אחר פעילויות חריגות/עויינות (ניסיונות הזדהות כושלים, גישה לא מורשית, ניסיונות כניסה כפולים ועוד).
- 14.9 הספק יספק מידע אודות תוצאות מבדקי חדירה המתבצעים באופן תדיר לפי סטנדרטים מקובלים על פי תקני אבטחת מידע.
- 14.10 אירועים שיוגדרו ברמת סיכון גבוה כגון חשד לנגישות זרה ו/או הזלגת מידע ממאגר הנתונים הספק יעדכן באופן מידי את נתיבי איילון (על פי רשימת תיוג מוגדרת) ויודיע את אופן הטיפול בהם.

15. מדיניות אבטחת המידע וההגנה אחידה לכל הלקוחות.

- 15.1 מידע של לקוחות לא יוצא מן המתקן החוצה שלא בדרך הלוגית שסוכמה עם הלקוח.
- 15.2 כלל העובדים אשר נגישים למידע לוקחות הינם עובדי החברה, לאחר בדיקות רקע וגיוס דקדקני.
- 15.3 הספק יידרש לקבל אישור מראש לגישה לטבלאות.

16. אחסון וגיבוי

- 16.1 הלקוח (נתיבי איילון) יקבע היכן מידע של הלקוח יישמר
- 16.2 תהליכי גיבוי – בכל אתר קיימת מערכת "זמן אמת" עליה מאוחסן המידע והן מערכת גיבוי אליה נדחף המידע אחת ליום.
- 16.3 הספק ידאג לגיבוי OffSITE.
- 16.4 שיחזור מידע העלאה מגיבוי – באחריות, ניהול והתפעול הספק. יש ליידע את הלקוח כי בוצע שיחזור מידע מגיבוי.

17. סיום התקשרות עם ספק

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

- 17.2 מחיקה חד חד ערכית ולא ניתנת לשחזור של כל הנתונים והמידע השמורים בשירות הענן ונמצאים תחת שליטת נתיבי איילון.
- 17.3 השמדת עותקים של הנתונים והמידע בהם נעשה שימוש במסגרת פעילות הספק עבור נתיבי איילון.
- 17.4 דרישה מהספק להציג הוכחות לכך שהמידע הושמד (רישומים ודוחות רלוונטיים).
- 17.5 במידה והמידע הוצפן – ביטול (Revoke) מפתחות ההצפנה ומחיקתם.