

מסמך ד' - דרישות אבטחת מידע – מכרז SIEMSOC As A Service

כללי

כחלק מהעבודה השוטפת בין נתיבי איילון לספקיה החיצוניים, נתיבי איילון מעבירה אל הספקים מידע ומידע רגיש (יקרא גם מידע סודי כחלק מההתקשרויות) לצורך ביצוע העבודה בהתאם להסכם ההתקשרות. מידע זה הוא רכוש (נכסי מידע) חברת נתיבי איילון ויש להגן עליהם מתוקף חוק הגנת הפרטיות, התשמ"א – 1981 והתקנות שמכוחו, וכמפורט בנספח זה. מידע רגיש בהתאם להגדרתו בחוק הגנת הפרטיות, התשמ"א 1981 - והתקנות שמכוחו.

מטרה

הגדרת דרישות אבטחת מידע לנכסי המידע של נתיבי איילון הנמצאים בחצרות ספקיה על מנת לוודא הגנה על המידע המאוחסן והמעובד אצל הספק.

שיטה

- על הספק לעמוד בדרישות האבטחה בנושאים הבאים:
- דרישות כלליות.
- משאבי אנוש.
- הפרדת פעילויות.
- אבטחה פיזית.
- אבטחת הרשת, התקשורת, המחשבים.
- בקרת גישה.
- העברת מידע.
- שימוש בענן.
- גיבויים.
- התאוששות מאסון והמשכיות עסקית.
- שמירת המידע.

דרישות כלליות

שמירת סודיות

על הספק לחתום על הסכם שמירת סודיות מול נתיבי איילון כחלק מהסכם ההתקשרות. על הספק לחתום בשם ו/או להחתים את כל העובדים המורשים לגישה למידע של נתיבי איילון, על אותו הסכם לשמירת סודיות מול הספק עצמו.

נהלים

באחריות הספק לוודא כי ההנחיות המפורטות להלן מעוגנות בנהלים הפנימיים שלו.
נהלים אלו יובאו לידיעת כלל העובדים אצל הספק העוסקים בפעילות הנוגעת לנתיבי איילון באופן ישיר ו/או עקיף.

ביקורות של נתיבי איילון בחצרות הספק

אחת לתקופה, בהתאם להחלטת נתיבי איילון, תבוצע בדיקת אבטחת מידע באתר הספק, בהודעה מראש של 14 יום לפחות. בבדיקה זו ייבדק בין היתר כי הספק מקיים את התחייבויותיו בנושאי אבטחת המידע, מערכות המחשוב של הספק וקיומם של תהליכי עבודה מאובטחים הנוגעים לנתיבי איילון.
הספק מחויב לתקן את הליקויים, במידה ונמצאו, בתוך פרק זמן אשר יוגדר בשיתוף עם נתיבי איילון.
לאחר סיום תיקון הליקויים, יודיע מידית הספק לנתיבי איילון כי הליקויים תוקנו.

סיום התקשרות עם ספק

עם סיום ההתקשרות של נתיבי איילון עם ספק יבוצעו הפעולות הבאות:

- החזרה של כל הנתונים והמידע אשר ברשות הספק לידי נתיבי איילון.
- הספק לא ישאיר עותקים של הנתונים והמידע בהם נעשה שימוש במסגרת פעילות הספק עבור נתיבי איילון כולל בשירותי ענן, גיבויים ותהליכי התאוששות מאסון.
- באחריות הספק להוכיח לנתיבי איילון כי הנתונים אכן הוסרו.

משאבי אנוש

הספק יפעל לשבץ ו/או לקלוט לעבודה הקשורה לנכסי המידע של נתיבי איילון עובדים המתאימים לעבודה זו, לאחר שנקט באמצעים סבירים ומקובלים בהליכי מיון עובדים ושיבוצם.
הספק יתחשב ברגישות המידע של נכסי המידע של נתיבי איילון ויסדיר בהתאמה את היקף ההרשאות והפעולות לביצוע שמורשה התפקיד שמיועד לו העובד המועמד לתפקיד.
הספק יבצע פעילות הדרכה בנושא החובות לפי חוק הגנת הפרטיות והתקנות בסמוך לחתימת הסכם ההתקשרות ותחילת העבודה לבעלי ההרשאות לנכסי המידע של נתיבי איילון וישמר את הידע בהדרכה תקופתית אחת לשנתיים לפחות.

הפרדת פעילויות

הספק יפריד את פעילות העיבוד המתבצעת עבור נתיבי איילון מפעילויות עיבוד אחרות המבוצעות על ידו.
עיבוד מידע של נתיבי איילון ושמירתו תבצע באמצעות מחשב ייעודי המופרד לוגית מהרשת הארגונית ומרשתות ציבוריות/אינטרנט.

באחריות הספק להקצות ספרייה נפרדת ייעודית שעליה יאוחסן המידע המעובד של נתיבי איילון.

אבטחה פיזית

הספק יקיים בכל עת נהלים ומדיניות להגנה ואבטחה פיזית של המידע ויציג אותם לחברה על פי דרישתה.

הספק יאחסן חומר פיזי (דפוס, קלטות גיבוי, מצעי מדיה) באזורים מאובטחים וממודרים.

הספק ימדר את הגישה הפיזית למידע של החברה (על בסיס הצורך לדעת/לעשות).

הספק יישם מנגנוני בקרת גישה פיזית באמצעות אמצעי הזדהות חד-ערכי.

הספק יאכסן חומר המגיע מהחברה ו/או מי מטעמם, בצורה מאובטחת לצילום 24/7 ויכולת תחקור של עד חודש.

הספק יבצע ביקורות אבטחה פיזית מעת לעת בתדירות משתנה ויפעל לתיקון הליקויים ושיפור הבקורות שיעלו במסגרת ביקורות אלה בדגש על הנושאים הבאים:

- אבטחת חדר שרתים וארונות תקשורת.
- באחריות הספק לוודא נעילת ארונות תקשורת.
- באחריות הספק לוודא נעילת חדר השרתים על ידי דלת קשיחה הניתנת לנעילה.
- באחריות הספק לקיים מנגנוני התרעה על גישת גורם שאינו מורשה לחדרי השרתים.
- באחריות הספק לקיים מנגנוני תיעוד כלל אירועי הגישה לחדרי שרתים.
- במידה וישנו חלון בחדר השרתים, על הספק להתקין סורגים על מנת למנוע גישה של גורם זר.
- באחריות הספק לקיים מנגנוני כיבוי אש, מיזוג אוויר ואספקת חשמל מתאימים ויתירים בחדרי שרתים.

אבטחת ציוד מחשוב וניירת

ספק אשר קיבל מנתיבי איילון מדיה מגנטית ישמור את המדיה בחדר או כספת נעולים הנגישים רק למורשים למידע זה.

המדיה המגנטית תושמד על ידי הספק מיד עם סיום הצורך לבצע שימוש בה.

ניירת המכילה נכסי מידע של נתיבי איילון תישמר בארון נעול ותהיה נגישה לגורמים מורשים בלבד.

באחריות הספק לקיים הליכי גריסת ניירת המכילה נכסי מידע של נתיבי איילון בתום השימוש בה.

סביבת העבודה של העובדים

סביבת העבודה על נכסי המידע של נתיבי איילון תהיה מאובטחת ותתאפשר גישה של העובדים המורשים בלבד.

ניהול אבטחת הרשת, התקשורת, המחשבים ומערכות אוטומציה ובקרה תעשייתיות

הרשת הארגונית של הספק תופרד לוגית מרשת האינטרנט ומרשתות ציבוריות אחרות באמצעות רכיב אבטחתי כדוגמת FW.

הרשת הארגונית תכיל רכיבי אבטחה כגון מערכת בקרת גלישה וכדומה למניעת סיכוני סייבר.

באחריות הספק לבקר חיבור אמצעי מדיה נתיקים ולאפשר חיבורם אך ורק עפ"י צורך ייעודי ולעובדים מורשים בלבד.

תפעול

אין לבצע תמיכה ותחזוקה במערכות הספק באמצעות גישה מרחוק שלא באמצעות תוכנה אבטחה ייעודית ומאובטחת.

על הספק לוודא כי ציוד המחשוב, המחשבים 'בכלל זה מחשבים ניידים/לוח, מכשירים חכמים התקשורת ומערכות ההפעלה הינם בגרסת העדכון האחרונה המפורסמת ע"י הספקים, הציודים והמערכות מוקשחים, ושהוגדרו ויושמו מפרטי הקשחה טרם תחילת ביצוע הפעילות.

באחריות הספק להתקין מערכת אנטי וירוס/EDR מעודכנת באופן תדיר על כל תחנות הקצה והשרתים.

בקרת גישה - אמצעי הזדהות

באחריות הספק לאפשר גישה לנכסי המידע של נתיבי איילון רק לעובדים המורשים למידע זה בלבד לצרכי עבודתם.

אמצעי הזיהוי לכניסה למערכות ושירותים של הספק יהיה מורכב מקוד משתמש חד-ערכי בין 4 ספרות לפחות ומסיסמא בעלת 10 תווים לפחות.

אמצעי הזיהוי של משתמשים בעלי הרשאות ניהוליות יבוצע באמצעות קוד משתמש חד-ערכי בין 4 ספרות לפחות וסיסמא בעלת 14 תווים לפחות.

על כלל הסיסמאות להיות מורכבות ממספרים, אותיות קטנות, אותיות גדולות וסימנים מיוחדים.

באחריות הספק לבצע החלפה של סיסמאות לפחות אחת ל – 90 יום.

יש לבצע שמירת היסטוריה של סיסמאות (לפחות 10 סיסמאות אחרונות).

יופעל שומר מסך מוגן סיסמא לאחר 15 דק' ללא פעילות בתחנת העבודה ממנה מתבצעת ההתקשרות.

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

ניהול הרשאות

אחת לתקופה מוגדרת יבצע הספק סקר/טיוב הרשאות ומשתמשים. במסגרת זו הספק יודא כי המשתמשים וההרשאות מוגדרות על פי עיקרון "הצורך לדעת". עיקרון זה מגביל את תפוצת המידע לבעלי התפקידים הזקוקים לו בלבד.

העברת מידע

העברת נכסי המידע של נתיבי איילון בין נתיבי איילון לספק תבוצע כאשר המידע מוצפן ומאובטח.

בהתאם להיקפי המידע ותכיפות ההעברה תועדף העברה באמצעות קווי נל"ן מוצפנים.

במידה ויועבר המידע באמצעות מדיה מגנטית כלשהי, המידע המועבר המצוי במדיה זו יהיה מוצפן.

לא יועברו נכסי המידע של נתיבי איילון באופן גלוי ע"ג רשתות ציבוריות.

כל העברת מידע בין נתיבי איילון לספק באמצעים קשיחים (נייר, מדיה נתיקה) תבוצע ע"י שליח המאושר על ידי נתיבי איילון.

חל איסור על הספק להעביר את נכסי המידע של נתיבי איילון לכול גורם שהוא מלבד הצורך לקיומם של הוראות דין מפורשות.

על הספק ו/או ספקי המשנה שלו מוטלת האחריות ללמוד, להכיר ולעמוד בחוק הגנת הפרטיות, התשמ"א 1981 והתקנות שמכוחו, כולל ובין היתר תקנות אבטחת המידע, ולפעול עפ"י הוראות החוק הנ"ל בכל עת שהם פועלים עם נכסי המידע של נתיבי איילון.

שימוש בענן

לא יבוצע שימוש בענן לעיבוד, אחסון ופעולות אחרות כלשהן ללא אישור מנהל אבטחת מידע של חברת נתיבי איילון.

ככל שידרש לבצע שימוש בשירותי ענן כלשהם בהם מעורבים נכסי המידע של נתיבי איילון הוא יבוצע בין היתר עפ"י העקרונות הבאים:

מידע רגיש ומידע רגיש עסקי/כספי יהיה בשירותי ענן המתקיימים בישראל בלבד.

כל מידע אחר בשירותי ענן שמחוץ למדינת ישראל יתקיים ובתנאי שהדין באותה מדינה מבטיח רמת הגנה על מידע שאינה פחותה מרמת ההגנה הקבועה בדין הישראלי, (מדינות ידידותיות בלבד) עם הסכמים משפטיים מתאימים ושאינן בעשיריה הראשונה של מדינות, מלבד ישראל, מהן יוצאות תקיפות סייבר.

המידע יוצפן בכל שלבי התהליך.

הנחיות אבטחת המידע הנ"ל בהתאמה הנדרשת ייושמו עם ספק שירותי הענן.

גיבויים

באחריות הספק לבצע גיבויים שוטפים לנכסי המידע של נתיבי איילון שבתחומיו ויקיים תהליכים לבדיקת תקינות הגיבויים אשר יבטיחו כי מתקיימת יכולת השחזור של המידע המגובה אך ורק עבור שימור היכולת לביצוע הפעילויות עם נתיבי איילון.

התאוששות מאסון והמשכיות עסקית

באחריות הספק לקיים מערכת ותהליכי עבודה אשר יאפשרו התאוששות מאסון והמשכיות עסקית אשר תאפשר המשך הספקת השירותים לנתיבי איילון בהתאם להסכמי ההתקשרות עמו.

שמירת מידע

הספק רשאי לשמור את נכסי המידע שהתקבלו מנתיבי איילון, או מידע שהספק צבר בעצמו אגב מתן השירותים, רק למשך פרק הזמן הנדרש במישרין לביצוע תפקידו לפי הסכם ההתקשרות.

סיום ההתקשרות

עם סיום ההתקשרות עם הספק, על הספק למחוק מכל אמצעי המדיה שברשותו, לרבות כוננים קשיחים, אמצעי גיבוי וכל מדיה מגנטית או אופטית אחרת את נכסי המידע שהתקבלו מנתיבי איילון.

ככל שקיימת הוראה בדין המחייבת שמירת המידע אצל הספק, הספק מחויב כי יבוצעו כל ההנחיות ויופעלו כל אמצעי האבטחה והבקרה שהוגדרו בהסכם ההתקשרות עם נתיבי איילון והם יישארו אפקטיביים לכל אורך תקופת השמירה.

עם סיום ההתקשרות עם הספק, על הספק למסור לנתיבי איילון תצהיר המאמת ביצוע פעולות מחיקה, ביעור והשמדה של כל המידע שהגיע אליו במסגרת הסכם ההתקשרות עמו.

אבטחת מידע בניהול כוח אדם

הספק יחתים את בעלי הרשאות מטעמו על הצהרות סודיות הכוללות, בין היתר, התחייבות לשמירה מוחלטת על סודיות המידע של נתיבי איילון שימוש במידע רק בהתאם לאמור בהסכם ההתקשרות בין הספק לנתיבי איילון ויישום אמצעי האבטחה הקבועים בהסכם ההתקשרות, לרבות נספח זה.

הספק ייתן וישנה הרשאות גישה למידע רק לאחר נקיטת אמצעים סבירים, המקובלים בהליכי מיון ושיבוץ עובדים.

הספק יקיים הדרכות לבעלי הרשאות גישה למידע הן באופן תקופתי והן בטרם מתן ההרשאות או בטרם שינוי ההרשאות הקיימות. ההדרכות יעסקו בחובות לפי חוק הגנת הפרטיות, התשמ"א (1981-) להלן: "החוק", תקנות אבטחת המידע, מסירת מידע, חובות בעלי הרשאות לפי החוק, נוהל האבטחה של הספק והסכם זה.

הגנה על מחשבי הספק המשמשים להתחברות למשאבי החברה

הגישה למערכות הניטור תתבצע באמצעות מנגנוני MFA.

שימוש במדיניות סיסמאות מורכבת מאותיות, ספרות, סימנים מיוחדים ואורך סיסמא מינימלי 8 תווים.

סיסמאות ניהול יהיו בנות 14 תווים לפחות.

החלפת סיסמאות לפחות כל 3 חודשים.

הגדרת מספר ניסיונות הקשה שגויים של סיסמא בטרם נעילת המשתמש.

הגדרת Out Time Session לאחר פרק זמן של אי פעילות, המחייב זיהוי מחדש של המשתמש.

ברירת המחדל לסיום Session תהיה 15 דקות (גם אם המערכת תנוהל מקומית).

הצפנת הסיסמאות בהצפנה חד כיוונית בבסיס הנתונים.

הגדרת אופן טיפול בתקלות הקשורות באימות זהות.

ביטול הרשאות לבעל הרשאה שסיים את תפקידו ובמידת האפשר שינוי סיסמאות למאגר ולמערכות המאגר, שבעל הרשאה עשוי היה לדעת, מיד עם סיום תפקידו של בעל הרשאה.

הספק יוודא שימוש במערכות הפעלה, דפדפנים, בסיסי נתונים ותשתיות תוכנה בגרסאות נתמכות בלבד.

לא ייעשה שימוש במערכות שהיצרן לא תומך בהיבטי אבטחה שלהן אלא אם כן ניתן מענה אבטחתי מתאים.

ניהול מאובטח ומעודכן

הספק יבצע הפרדה לוגית בין המידע של נתיבי איילון לבין מידע של לקוחות אחרים.

זמינות מרבית – הספק יזווח לנתיבי איילון על כל השבתה של המערכת.

הספק ישמור את המידע כל עוד נמשך השירות.

התקשורת בין נתיבי איילון לספק תבצע באמצעות כתובות IP שהוגדרו מראש לספק. תווד התקשורת בין נתיבי איילון לספק יהיה מוצפן עבור כל השירותים הקיימים.

ממשק ניהול בגישה מהרשת בלבד או מכתובות שיסופקו על ידה.

במקרה של ניהול בענן – מימוש אמצעי ניטור והגנה על תשתיות ענן, בין היתר :

1. הצפנת המידע במנוחה, תנועה ועיבוד.
2. מנגנון ניהול זהויות, הרשאות וגישה.
3. ניטור תשתית הענן לגילוי, זיהוי וחסידת מתקפות.
4. יכולת גיבוי ושחזור נתונים.
5. מדיניות עדכונים וניהול שינויים.
6. אמצעי אבטחה כגון, VPN, FW, WAF, Anti-Bot, CASB, IPS, EDR וכיו"ב.

מימוש הצפנה בתקשורת באמצעות פרוטוקול TLS 1.2 או פרוטוקול אחר שיאושר ע"י גורמי אבטחת המידע של נתיבי איילון או קו ייעודי בין הספק לחברה.

הספק יספק לנתיבי איילון יכולת שליטה ובקרה על הנתונים שלה וכן אפשרות חד צדדית להפסקת השימוש בשירותים תוך השבת כל המידע של החברה לידיה.

המידע הקיים ברשתות המזמינה הינו מידע רגיש בהיבט של צנעת הפרט וסודיות עסקית. בהתאם לכך נדרש יישום אבטחת מידע במערכת ומידור מלא של המידע אשר ייבחו ויאושר מראש ע"י גורמי אבטחת המידע בנתיבי איילון.

ניהול הרשאות גישה למערכת ולישויות השונות יהיה על בסיס עיקרון הגישה המינימלית הנדרשת לבצע את המשימה, תוך הקפדה על מידור מלא.

העברת מידע לגורמי צד שלישי, ובכללם גורמי אכיפת חוק וואו גורמי ממשל כדוגמת מערך הסייבר, דורשת אישור מפורש נתיבי איילון טרם ביצוע הפעולה. העברת מידע על פי חוק ובכללו על פי צו בית משפט, תדווח לנתיבי איילון, אלא אם קיים צו איסור פרסום המונע את העברת הבקשה לנתיבי איילון.

לא תינתן גישה לכל גורם צד שלישי כלשהו למערכת SOC/SIEM שלא באישור נתיבי איילון בכתב, תוך ציון מדויק וברור של צורך ונתונים אליהם יש צורך לגשת, אם לצורך פתרון בעיה במערכת SIEM או לניתוח מידע שעלה מהמערכת.

בפתרון מנוהל הכנסת שינויים במערכת SIEM או תשתית SOC הנלווית אליה תעשה על ידי בעלי תפקידים מוגדרים ומורשים על ידי הספק ונתיבי איילון בלבד. כל פעילות שהיא חריגה להקמת מערכת SIEM או תפעולה השוטף תדווח ותקבל את אישור נתיבי איילון טרם ביצוע הפעילות.

בפתרון SIEM בתצורת SaaS

לא תינתן גישה לכל גורם צד שלישי כלשהו למחיצת Tenant של נתיבי איילון שלא באישור בכתב, תוך ציון מדויק וברור של הצורך והמידע אליו יש לגשת.

הכנסת שינויים ברמת Tenant תעשה אך ורק באישור נתיבי איילון מראש ובכתב, תוך כדי ציון מדויק של השינוי, הסיבה לשינוי, השפעתו והסיכונים הכרוכים בביצוע או באי ביצוע השינוי.

כללי

הספק יגדיר איש קשר, אשר יהווה רפרנט למול החברה, שפרטיו והדרכים ליצירת קשר עמו ושזהותו תאושר על ידי החברה.

הספק ישתף פעולה עם סקרי בטיחות ויעמוד בלוחות הזמנים שייקבעו לתיקון הליקויים שימצאו בסקרי הבטיחות כאמור.

הספק ועובדיו וכן ספקי צד ג' (ספק של ספק) הניגשים למידע של החברה – יחתמו על הסכם סודיות.

הספק יקיים נהלי אבטחת מידע שיכללו בין השאר :

- הקצאת הרשאות ובקרתן
- אחריות העובד לאבטחת מידע

ויציג את הנהלים לחברה על פי דרישתה מעת לעת.

הספק יקיים מדיניות הערכת סיכונים ותכנית עבודה לטיפול בפערי אבטחת המידע, ויציג אותה לחברה לפי דרישתה.

הספק יעביר על פי דרישת החברה רשימה של כלל העובדים המורשים על ידו בביצוע השירותים לרבות עובדי תשתיות ומערכות מידע הנחשפים למידע.

הספק יקיים תכנית לשמירה והעלאת מודעות עובדים לנושאי אבטחת מידע בדגש על עובדים הניגשים למידע של החברה ויציג לחברה את התכנית כמו גם אסמכתאות למימושה בפועל, על פי דרישתה.

ספק המחזיק מאגר מידע או חלק ממאגר מידע, יקיים את דרישות אבטחת המידע במאגרים בהתאם לדרישות הדין והוראות כל רשות מוסמכת בנושא.

שמירה על מידע

הספק יקיים נהלים ומדיניות להגנה מפני דלף מידע ויציג אותם לחברה על פי דרישתה מעת לעת.

הספק יגן על מידע של החברה בעת שינוע המידע ובעת אחסון המידע.

הספק יקיים העברת מידע של החברה ו בצורה מאובטחת, ע"ב שימוש במערך הכספות ו/או שיטה להעברת מידע מאובטחת.

במידה והספק מחזיק מאגר מידע של החברה, עליו לבצע הפרדה בין מידע זה למידע של ארגונים אחרים.

הספק יקיים נהלים להשמדה של מדיה מגנטית ואופטית לרבות כוננים קשיחים, אמצעי אחסון

ניידים או נתיקים, מצעי גיבוי וכד' בסיום ההתקשרות עם החברה.

הספק לא יבצע כל פרסום של מידע הקשור לחברה אלא אם לכך אישור מראש ממחלקת אבטחת מידע.

אבטחה לוגית

הספק יישם הגנה לוגית על מערכות המחשוב, תוכנות התשתית, רכיבי הרשת, התוכנה הקבצים ומסדי הנתונים.

הספק לא יאחסן או ינייד מידע של החברה במצעי מדיה נתיקה (CD, Key On Disk) כונן קשיח נייד) או באמצעי

מחשב נייד (מחשב נישא, טלפון נייד, טאבלט) ללא הצפנה חזקה של מצע המדיה או המחשב הנייד.

הספק יישם אמצעים לגילוי, התרעה והסרה של וירוסים ותוכנות זדוניות בכל סביבות העבודה.

הספק יקיים הפרדה בין סביבת הייצור לבין סביבת הייצור והפיתוח ובין סביבות בהן קיים מידע של החברה

לבין סביבות מידע שאינן של החברה.

הספק יקיים פעולות לאבטחת תשתיות התקשורת, בין השאר יפריד בין רשת התקשורת הפנימית בה מעובד

מידע השייך ו/או הנוגע לחברה ו/או מקושר למערכותיהם, לבין סביבת האינטרנט.

חיבור לרשת האינטרנט יתקיים באופן מאובטח, בין ע"י ארכיטקטורה ובין ע"ב טכנולוגיה ייעודית לנושא.

חיבור עובדים לעבודה מהבית יתקיים רק בעת הצורך, במקרים חריגים (מצבי חירום) ובאמצעים אשר יאושרו

מראש ע"י נתיבי איילון.

בכל אופן לא תתקיים לגישה למידע של החברה בגישה חיצונית.

הספק יבטיח כי בכל גישה מרחוק למערכות המחשוב שלו (עובדים ו/או ספקים צד שלישי) תעשה בתצורה

מאובטחת הכוללת:

- הצפנת תווך.
- ניהול קבוצות הרשאה.
- בקרה אחר פעולות המשתמשים.
- שימוש באמצעי חציצה (דוגמת שרת טרמינל).

במידה וקיימת רשת אלחוטית, הספק יוודא כי תצורת השימוש ובקרת הגישה אליו נעשית באופן מאובטח. בכל

מקרה אין לבצע שימוש ברשת אלחוטית בטיפול במידע או בגישה למידע של החברה.

הספק יעדכן את מערכות המידע שלו בעדכוני תוכנה ומוצרי אבטחת מידע.

הספק אחראי לכך כי לא יחובר התקן נייד שלא עבר בדיקה, למערכות המחשוב בו נשמר מידע

של החברה.

קבלני משנה (ספק של ספק)

הספק אחראי לקיום כל התחייבויותיו לשמירה על גם אצל קבלני משנה מטעמו, ככל שישנם ואלו אושרו על ידי החברה, לרבות החתמה על טופסי שמירת הסודיות כפי המקובל בהחברה.

הספק יעדכן את החברה על כל גישה של קבלן משנה (שאינו הספק הישיר, לדוגמא ספקי תחזוקה) בגישה או ביכולת אפשרית לגישה למידע של החברה.

הספק יקיים מנגנון בקרת גישה של קבלני משנה, למידע של החברה למידע כאמור הנמצא במערכות של הספק. מנהל אבטחת המידע של החברה יהיה הגורם שיאשר מראש כל גישה קבלן משנה למידע של החברה.

חיבור קבלני משנה, יאושר באופן פרטני ע"י אבטחת מידע של החברה תוך קיום ההנחיות של החברה.

בכל אופן לא תתקיים לגישה למידע של החברה בגישה של ספקים צד ג' ללא אישור החברה.

טיפול באירועי אבטחת מידע

על הספק להציג לחברה, על פי דרישתה, מוכנות לטיפול באירועי אבטחת מידע, בין השאר בקיומם של מסמכי מדיניות ונהלים לטיפול באירועים.

הספק ימנה נציג שיהיה אחראי על טיפול באירועי אבטחת מידע (ניתן לעשות שימוש בשירותי צד שלישי) ופרטי הנציג והחברה השלישית יועברו לחברה מראש ובכתב.

על הספק לדווח לחברה, בעל פה ובמקביל גם בכתב, על כל אירוע אבטחת מידע המתרחש אצלו בחברה, תוך 3 שעות.

הספק ייצר, יגן ויתחזק היסטוריה של לוגים ממערכות המחשוב שלו, תוך שמירה על היכולת לנטר, לנתח ולבצע תחקור על אירועי אבטחת מידע. בנוסף הספק יבטיח כי כל פעילות המשתמשים מטעמו תנוטר באופן שיהיה ניתן לאתר את המשתמש שגרם ו/או שמעשה ו/או מחדל שלו גרמו ו/או אפשרו את האירוע.

במקרים בהם מחלקת אבטחת מידע בחברה או מי מטעמה יעבירו לספק מידע בנושא איומי סייבר, יפעל הספק לקיום בקורות מפצות ויעדכן את החברה בגין הבקורות אותן הוא מבצע.