נספח – דרישות אבטחת מידע

ⓘ על הספק להתייחס לכל סעיף ותת סעיף בנספח זה ולפרט על אופן עמידתו בנדרש בו.
ⓘ נשמרת הזכות ללקוח לקיים מפגשי F2F הן מול הספק בארץ ובחו"ל

1.1 מערכות ותשתיות המוקמות באתר חיצוני ו/או מבוססות על פלטפורמה בענן נדרשת להיות בעל יכולות אבטחה והגנה מפני איומים במערכות ובתשתיות אופן שמוגדר בסעיפים להלן.

1.2 דרישות אבטחת המידע חלות על כל מחזור החיים של הפרויקט והמערכת (לרבות הפלטפורמה), וכן על מערכות נוספות אם יוזמנו ע"י חברת הדואר, ויהיו תחת אחריות הספק ובפיקוח של חברת הדואר, ובאות לתת מענה לנושאים הבאים:

1.2.1 <u>איומים</u>

- **איום פנימי** - פגיעה במכוון או בשוגג בנכסי הדואר וכן בשלמות, זמינות ו/או סודיות של נכסי המידע של חברת דואר ישראל על ידי גורם בעל הרשאות גישה לאותם נכסים.
- **איום חיצוני** - פגיעה במכוון או בשוגג בנכסי הדואר וכן פגיעה בשלמות, זמינות ו/או סודיות של נכסי המידע של חברת דואר ישראל על ידי גורם ללא הרשאות גישה מאושרות לאותם נכסים.

1.2.2 <u>גורמי איום עיקריים</u>

- אדם בעל הרשאות במערכת וללא הרשאות במערכת.
- בעל עניין במידע (אדם/ ארגון/ מדינה).
- גופים עם אינטרסים ועם יכולות – אנשי תקשורת, חוקרים פרטיים, עבריינים קטנים, פשע מאורגן ישראלי ופשע מאורגן בינלאומי.
- אדם אקראי או גורם נוסף בעל יכולת זדונית.

1.2.3 <u>מימוש האיומים ופגיעה בנתוני המערכת, עלולים לגרום לנזקים הבאים:</u>

- פגיעה בפעילות התקינה בחברת דואר ישראל כולל זמינות שירותים, אמינות שלמות וחסינות נתונים.
- פגיעה בצנעת הפרט של עובד חברת הדואר או של אדם מן הציבור ו\או לכל לקוח של חברת הדואר לרבות תאגיד ו/או אדם שפרטיו נחשפו מהמערכת.
- חשיפה לתביעות משפטיות נגד חברת דואר ישראל.
- נזק כלכלי לחברת דואר ישראל.
- נזק לטובין.
- נזק למידע.

1.3 <u>הצפנה וחתימה</u>

1.3.1 על המערכת ומרכיביה (לרבות הפלטפורמה) לכלול יכולות הצפנת מידע וחתימת השדרים (חתימה דיגיטלית).

1.3.2 יש להשתמש בהצפנת סיסמאות.

1.3.3 הצפנת שדות רגישים בבסיס הנתונים

1.3.4 הצפנת תווך התקשורת, כלומר: בתוך המערכת עצמה, בין המערכת אל הפלטפורמה, בין הפלטפורמה אל המערכת, ובין המערכת למערכות נוספות הפועלות בחברת הדואר כיום ו/או מערכות נוספות ככל שיוזמנו ע"י חברת הדואר מהספק לפי ההסכם, בתקן הצפנה עדכני.

1.3.5 עבור ממשקים שיש להם משמעות משפטית, על הספק להתייחס למנגנוני מניעת התכחשות.

1.3.6 על הספק לפרט את פתרונות אבטחת תעבורת המידע בכלל במקרה של מתקפת סייבר בפרט.

1.3.7 מפתחות ההצפנה צריכים להישמר בחצרי דואר ישראל בלבד ולא לעבור ליצרן בחו"ל.

1.4 <u>זיהוי וניהול סיכונים</u>

1.4.1 הספק מתחייב לבצע ניהול וזיהוי של סיכוני אבטחת מידע בכל שלב משלבי הפרויקט.

1.4.2 הספק ימציא לחברת הדואר אישורים על רמת חוסן המערכת והפלטפורמה מפני תקיפות סייבר ובכלל זה אישורים על בדיקות חדירה ותוצאותיהם. האישורים יומצאו פעם ראשונה במסגרת ההצעה, ולאחר מכן במהלך תקופת ההתקשרות, מעת לעת על פי דרישה או לאחר אירועי תקיפות סייבר, לרבות פירוט המלצות ואמצעים שננקטו לפתרון. הספק מודע לכך שחברת הדואר תהא רשאית לערוך בדיקות חדירה על מנת וודא עמידתו של הספק בדרישות אבטחת המידע נשוא פרק זה. הספק מתחייב לשתף פעולה עם חברת הדואר לשם כך באופן שיידרש על ידה. למען הסר ספק, מובהר כי כל זכות שניתנה לחברת הדואר לפקח, להדריך, להנחות ו/או להורות לספק ו/או למורשים (כהגדרתם להלן), ניתנו כאמצעי הגנה על בלבד ולא תתפרש, בשום מקרה, כמטילה על חברת הדואר חבות או אחריות כלשהיא המוטלת על הספק.

1.5 <u>אבטחה פיזית</u>

על הספק חלה האחריות לעשות שימוש באמצעים פיזיים נדרשים לצורך הגנה על כלל רכיבי המערכת, לרבות הפלטפורמה על כל רכיביה, על מנת למנוע זליגתם ו/או חשיפתם של נתוני חברת הדואר בפני גורמים שאינם מורשים ו/או לצורך מניעת ניצול לרעה של נתונים אלה, וכן על הגישה למידע של חברת דואר ישראל ולשרידות המערכות הנוספות אשר הספק יידרש לספק במסגרת החוזה, ולהתממשקות אליהן .

1.6 אבטחה לוגית

1.6.1 הספק מתחייב ליישם אמצעי אבטחה לוגיים/מיגוניים הולמים שימנעו חדירה מכוונת או מקרית למערכת והפלטפורמה ולמערכות הנוספות אשר יוזמנו ע"י חברת הדואר (ככל שיוזמנו). בכלל זה על הספק ליישם מנגנוני אבטחה על פי המאפיינים הבאים:

i. האימות יבוצע הן ברמת מערכת ההפעלה (כגון כלפי Domain) והן כלפי המערכת.

ii. על הספק לספק מנגנוני לנעילה זמנית של גישה במקרה של ניסיונות גישה כושלים רצופים בפרקי זמן קצרים.

iii. המערכת תאפשר היררכיה של משתמשים (לדוגמא: משתמש, מנהל, וכו').

iv. המערכת תאפשר הרשאות גישה ישירות שונות למשתמשים השונים.

v. על הספק חלה האחריות לצמצם למינימום הנדרש את השירותים המאופשרים כברירת מחדל (סוגים שונים של שירותי ניהול: SNMP, Telnet וכו').

vi. עדכוני תוכנה יבוצעו ע"י זיהוי חזק של המעדכן ובצורה מאובטחת. העדכונים ינוסו בסביבת טסט בטרם התקנתם בסביבת ה- PROD ויהיו חתומים ע"י היצרן.

vii. הספק יפרט את הרכיבים השונים שייושמו ואת הגדרות האבטחה ברכיבים השונים בהתאמה להגדרות לעיל.

1.6.2 על הספק לפרט את פתרונות אבטחת המידע למניעת שיבושים ו/או פגיעה בתפקוד המערכת על רכיביה, ותעבורת המידע בה, ממנה ואליה.

1.6.3 הספק יתחייב למנוע גישה למערכות המחשוב (בין אם של חברת הדואר, בין אם של הספק או של כל גורם אחר), בהן נשמר מידע הקשור למתן השירותים על פי הסכם זה, ממי שאינו מורשה ואושר על ידי קב"ט חברת דואר ישראל.

1.7 ניהול משתמשים והרשאות:

1.7.1 על הספק חלה האחריות על קיום מנגנון לניהול המשתמשים וההרשאות במערכת ובאחריותו לוודא כי ניהול המשתמשים וההרשאות מוגן מאובטח ומנוטר בהתאם לדרישות פרק זה.

1.7.2 הספק מתחייב שאפשרות הגישה אל המערכת ובכלל זה לכל בסיס הנתונים המצוי בה תהיה למורשים (כהגדרתם להלן), המבוססת על בסיס הצורך לדעת (need to know) בלבד, ולא תורשה גישה מעבר לנדרש לצורך מילוי התפקיד כפי שהוגדר על ידי חברת דואר ישראל ובהתאם להסכם. הספק ינחה וידריך את המורשים באופן שוטף בקשר למטרות השימוש בנתונים, ויהא אחראי לכך שהמורשים יפעלו בהתאם לתנאים בפרק זה.

1.7.3 הספק מתחייב לקיום מנגנון רישום מתעדכן של בעלי התפקידים ושל הגישה המוגדרת לכל תפקיד (לעיל ולהלן: "המורשים").

1.7.4 הספק מתחייב לגרוע הרשאות למורשים שהסתיים תפקידם או שאין להם צורך במידע אליו קיבלו הרשאה.

1.7.5 הזדהות ואימות משתמשי המערכת ב- Onprem יבוצע מול AD.

1.7.6 הספק מתחייב לדאוג לבקרות המתאימות על מנת שלא תבוצע גישה לא מורשית לאף אחד מרכיבי המערכת המוצעת במסגרת ההסכם.

1.7.7 הספק ינהל את תהליך הזדהות המשתמשים למערכת בצורה מאובטחת ומבוקרת. וייתן מענה לכלל התרחישים העולים במסגרת תהליך הזדהות המשתמשים שיש בהם כדי לפגוע ו/או לחבל בתפקוד המערכת ו/או השרות שניתן באמצעותה למשתמשים. בכלל זה, על המערכת להיות גמישה בפתרון ההזדהות ועליה לספק פתרונות שונים על בסיס התנאים:

- Something you have
- something you know

1.8 User Interface

הספק אחראי על אבטחת המידע בסביבת ממשק המשתמש ובאחריותו לספק מענה לסיכונים והאיומים בסביבה זו.

1.9 אבטחה אפליקטיבית

1.9.1 הספק אחראי לאבטחת המערכת ברמה האפליקטיבית ויבצע כל שנדרש כדי למנוע פגיעה במערכת, כגון: ביצוע סינון לכל פרמטר בכדי למנוע התקפות סייבר, המערכת תבצע בדיקת קלטיים למניעת התקפות ידועות באמצעות ממשקי קלט ובדגש על ממשקי קלט המועברים/מעדכנים בסיס נתונים וכיוצא בזה.

1.9.2 המערכת תאפשר משלוח התיעוד באופן אוטומטי למערכות איסוף נפוצות כגון: Windows event viewer ,syslog

1.9.3 תיעוד אירועים ייכתב בפורמט מקובל וסטנדרטי, מבנה הרשומות יהיה מובנה ונוח לקריאה ולניתוח ממוכן .

1.9.4 הספק יפרט בהצעתו את מנגנוני האבטחה באפליקציה.

1.10 מאגרי מידע

1.10.1 מבלי לגרוע מהוראות החוזה (ובפרט הוראות סעיפים 5.11, ו- 20 לחוזה), על הספק לעמוד ולקיים את כל הוראות חוק הגנת הפרטיות, התשמ"א-1981 (להלן: "**חוק הגנת הפרטיות**") (ובפרט פרק ב' – הגנה על הפרטיות במאגרי מידע), התקנות שהותקנו מכוחו, וכן לעמוד בדרישות הרשות למשפט טכנולוגיה ומידע (רמו"ט) משרד המשפטים כפי שיהיו בתוקף מעת לעת, ובכלל זה בהנחיות "שימוש בשירותי מיקור חוץ לעיבוד מידע אישי" שמפורסמות בכתובת: http://index.justice.gov.il/Units/ilita/faq/Documents/1122011.pdf. חל איסור מוחלט על הספק לאסוף מידע בדרכים בלתי חוקיות או לעשות שימוש במאגר מידע בלתי חוקיים.

1.10.2 על הספק חל איסור להעביר לצד ג' כלשהו מידע שיקבל במסגרת התקשרות זו לעשות כל שימוש במידע שאליו נחשף אגב ביצוע הסכם זה, לכל מטרה אחרת שאינה קשורה באופן ישיר לביצוע התחייבויותיו במסגרת ביצוע הסכם זה.

1.10.3 במהלך ביצוע הפעילות בהסכם הספק מתחייב לדאוג לאבטחת כל החומר שיגיע אליו במסגרת ביצוע פרויקט זה ולהציג לחברת הדואר, על פי דרישתה או דרישת מי מטעמה של חברת הדואר את אמצעי אבטחת החומר.

1.10.4 הספק מתחייב שלא לשמור ולא להוציא מידע במסגרת ההתקשרות עם חברת הדואר אל שרתים או משאבי מחשוב אחרים או שונים מאלה אשר נקבעו במסגרת ההסכם או ההתקשרות. המידע ישמר בשרתים במדינת ישראל או באיחוד האירופאי בלבד. אם מבוקש כי המידע ישמר, באופן קבוע או זמני, בשרתים שאינם במדינת ישראל או באיחוד האירופאי, אזי הסכם היצרן צריך לכלול התחייבות מפורשת כי יחולו הוראות הדין הישראלי על שמירת המידע ואחסונו (בחו"ל).

1.10.5 ככל שהדבר נדרש לפי הדין בישראל, תרשום חברת הדואר את הספק ו/או היצרן כמחזיקים במאגרי המידע של חברת הדואר, והספק ישתף פעולה עם חברת הדואר וימציא לחברת הדואר את כל הנתונים והמידע הדרושים לשם הדיווח עליו כמחזיק במאגר מידע אצל רשם מאגרי מידע. מבלי לגרוע מהאמור לעיל, באחריות הספק כי יקויימו על ידו ועל ידי היצרן כל הוראות הדינים הזרים החלים במדינות בהן מאוחסן המידע ו/או פועלים המציע והיצרן, לרבות ובמיוחד לעניין הגנת פרטיות ואבטחת מידע.

1.10.6 הספק ועובדיו יידרשו לחתום על התחייבות לשמירת סודיות ואבטחת מידע מול הדואר. עובדי הספק, ובכלל זה מנהל הפרויקט והגורמים שיחשפו למידע של חברת הדואר ימלאו ויחתמו על שאלון אישי, ויאושרו מראש ע"י חברת הדואר.

1.11 <u>ניהול אבטחת מידע</u>

1.11.1 הספק מתחייב כי בצוותי התמיכה והתגובה מטעמו יהיו נציגים בעלי ניסיון של מעל 5 שנים בתחום אבטחת המידע ובעלי הסמכה של CISSP ובעלי ניסיון של 3 שנים לפחות באבטחת מידע בענן ובעלי הסמכה של CCSK.

1.11.2 בכל מקרה שבו לספק התקשרות עם צד שלישי כלשהו אשר יש לה נגיעה עם ההתקשרות בין הספק לחברת הדואר במסגרת הסכם זה ו/או על יישום ההנחיות המפורטות במסמך זה, הספק מתחייב להודיע על כך לחברת דואר ישראל ולפעול על פי הנחיותיו וכן ליידע את הצד השלישי על החובות הנובעות מקיום ההנחיות המפורטות במסמך זה.

1.12 <u>אבטחת המערכת</u>

1.12.1 הספק ייתן מענה כולל לאבטחת מסדי הנתונים שהמערכת תעשה בהם שימוש בין במישרין ובין בעקיפין.

1.12.2 הספק מתחייב שהוא, או מי מטעמו, לא יעביר מידע, או חלק ממידע, מתוך מסדי הנתונים אשר בידיו או שיש לו גישה אליהם במסגרת התקשרות זו, לצד שלישי כלשהו ללא אישור מפורש ובכתב מאת חברת דואר ישראל.

1.12.3 על הספק חלה האחריות לאבטח, למדר ולנטר את מסדי הנתונים אשר יעשה בהם שימוש במסגרת הסכם זה מפני פגיעה והתממשות האיומים כפי שתואר לעיל.

1.12.4 על הספק להציג התהליכים והנהלים להגן על נתונים מפני פעילות לא רצויה. בכלל זה, יופעלו התקני אבטחה נוספים ברשת המתריעים על פרוטוקולים של תעבורה מאתרים זדוניים וכוללים זיהוי חדירה של אפליקציות וכלי פריצה.

1.12.5 הספק יפעיל ניטור אירועי אבטחת מידע על המערכות הקשורות לפעילות הדואר. הספק יתעד, ישמור ויסווג את האירועים לפי סוגים ורמות קריטיות וידווח למנהל אבטחת המידע בחברת הדואר על כך.

1.12.6 הספק יספק מנגנוני מיסוך וערבול נתונים עבור שדות רגישים.

1.12.7 הספק יבצע סקירות ומבדקים למציאת חורים ונקודות תורפה דרכן ניתן לפרוץ למערכת, וידווח למנהל אבטחת מידע בתוצאות.

1.12.8 המערכת תתממשק למערך הגיבויים והספק ישתתף בבדיקות תקינות הנתונים בשחזורים תקופתיים.

1.13 **<u>לוגים - רישום ללוג על כל פעולה, ושאילתה רגישה:</u>**

1.13.1 על הספק חלה האחריות לתת מענה כולל ומאובטח לתהליך תיעוד ורישום כלל האירועים (Auditing) במערכות הספק הרלוונטיות לשירותים המבוצעים ע״י הספק במסגרת ההסכם, לאורך כל שלבי ההתקשרות.

1.13.2 על הלוג להכיל נתונים שונים כגון: תאריך ושעה, שם תחנה/כתובת/מספר הכר, פירוט הפעילות, מיקום GEO ,שם משתמש, וכדומה.

1.13.3 על הלוג להיות חתום.

1.13.4 ניסיונות הכניסה למערכת, בין אם מוצלחים או לא, וכן יציאות מהמערכת יתועדו.

1.13.5 לוג על פעילות משתמשים ופעילות מנהלנים.

1.13.6 שינוי הגדרות.

1.13.7 אפשרות שליחת התראה על אירועים חריגים למערכות שו״ב וליעדים אחרים, לרבות אמצעים חיצונים (מייל, SMS).

1.14 **<u>אבטחה פרואקטיבית</u>**

1.14.1 על הספק לספק יכולות ניטור ואבטחת המערכת בזמן אמת מפני איומי סייבר שונים בין אם על ידי גורמים פנימיים של הספק ובין עם על ידי גורמים חיצונים והגנה על השירותים שיסופקו לדואר במסגרת הסכם זה באמצעות המערכת, וקבלת התראות בגין ניסיונות התחזות, מניעת שירות וכיוצא בזה.

1.14.2 הספק נדרש לדווח באופן מידי לחברת הדואר עד 8 שעות ממועד האירוע על כל תקלה או אירוע בנושא אבטחת המידע לרבות, דליפת מידע או שימוש חורג מההרשאה שניתנה או חשש לפרצת אבטחה ו/או דליפת נתונים. במקרה זה, על ספק לפעול לאלתר למניעת התממשות מתקפות סייבר וכל נזק כתוצאה

מהמתקפה ו/או התקלה.

1.14.3 על הספק לתעד כל אירוע אשר יש בו משום פגיעה בשלמות, סודיות וזמינות המידע ולדווח על כך למנהל אבטחת המידע של חברת דואר ישראל.

1.14.4 כל אירוע אבטחה, ייחקר וייבדק ע"י הספק ויופק דוח אירוע מפורט המתאר את הגורמים לאירוע ואת דרכי הטיפול באירוע. הספק יוציא הנחיות לביצוע על מנת להפחית את הסיכוי לאירוע דומה, ויפעל לשם כך בין היתר בהתאם להנחיות חברת הדואר.

1.14.5 על הספק להכין הוראות ונהלים להתמודדות עם אירועי סייבר ואבטחת מידע שונים תוך התייחסות לחומרת האירוע ולמידת רגישות המידע. בהוראות אלו תהיה התייחסות לצעדים מיידים הנדרשים לטיפול באירוע, אנשי קשר, וכדומה.

1.15 <u>פיתוח של המערכת ו/או מערכות נוספות אשר יפותחו על ידי הספק (ככל שיוזמנו)</u>

1.15.1 על הספק חלה האחריות כי פיתוח המערכת ועדכוניה (לרבות פיתוחים, התאמות, ממשקים, ושינויים – ככל שיוזמנו ע"י חברת הדואר) יבוצעו בכפוף לנוהלי הפיתוח המאובטח של דואר ובהתאם לדרישות תקני הפיתוח המאובטח (SSDLC) המקובלים כגון: OWASP. כמו כן, על הספק חלה החובה לבצע בדיקות מקיפות לזיהוי ומניעת סיכונים העלולים לנבוע בעקבות חורים ברמת הפיתוח והקוד.

1.15.2 יובהר כי בהתאם לנהלי הדואר, חלק מהותי מתנאי הקבלה של מערכת מידע היא ביצוע סקר ו/או בדיקות חדירות Penetration testing על ידי צד שלישי המתמחה בכך.

1.16 <u>רגולציה</u>

1.16.1 בנוסף על התחייבויות הספק המפורטות בסעיף 1.10 לעיל, על הספק לעמוד, בין היתר, גם בדרישות הרגולציה במסגרת היותו ספק נותן שירות ולעמוד בדרישות הרגולטוריות הנובעות מ- SSAE 16 (SAS70) ובכלל זה עמידה ב- SOC2.

1.16.2 על הספק לעמוד בתקן ISO 27001

1.16.3 על הספק לעמוד בתקן SOX

1.16.4 על הספק לעמוד בתקן PCI-DSS בכל מקרה של שימוש כרטיסי אשראי.

1.17 <u>תמיכה והתקנות</u>

1.17.1 ההתקנות תכלולנה את כלל מוצרי התוכנה לאבטחת מידע שישמשו בפרויקט, מקצה לקצה, בכל אחד מהרכיבים המרכיבים את המערכת, לרבות הפלטפורמה.

1.17.2 התקנות מוצרי התוכנה בתחום אבטחת המידע תכלול את גרסאות התוכנה העדכניות ביותר, ואת כלל ה-Hot fixes/Service Packs/Patches שיצאו למוצרי אבטחת המידע (מבוסס תוכנה בלבד או מבוסס חומרה ותוכנה) .

1.17.3 באחריות הספק להתקין את כלל עדכוני התוכנה בהקדם האפשרי לאחר פרסומם הרשמי כמפורט בסעיף זה תוך בדיקתם בסביבת טסט ואישורם בטרם הפצתם

בסביבת ה- PROD . כולל צד שלישי כמו Adobe shockwave

1.17.4 הספק מתחייב לתקן כל בעיה בתוכנה / חומרה שהתגלתה עקב עדכוני אבטחת מידע / פרצות אבטחת מידע במערכת כולל אלה של יצרנים כגון: מיקרוסופט.

1.17.5 באחריות הספק לספק פתרון אבטחתי מוסכם על חברת הדואר לאופן מתן התמיכה על המערכת.

1.17.6 המערכת תתמוך ביישום התקנות הנדרשות מכוח חוק הגנת הפרטיות, , התקנות שהותקנו מכוחו והנחיות הרשות למשפט טכנולוגיה ומידע, כפי שיהיו בתוקף מעת לעת.

1.17.7 חברת דואר ישראל רשאית, בכל עת, לבדוק את מערכות המידע של הספק התומכות בתהליך העבודה של הדואר. על הספק לפעול בשקיפות ולהעמיד לרשותה ועיונה של חברת דואר ישראל ו/או נציג מטעמו את כל החומר והמידע שידרשו ע"י חברת הדואר ו/או נציגה, עפ"י שיקול דעתה הבלעדי של חברת הדואר ו/או נציגה.

1.18 <u>תיעוד</u>

1.18.1 מבלי לגרוע מהתחייבויות הספק למסירת תיעוד עפ"י ההסכם, באחריות הספק להגיש תיעוד מפורט ומסודר, בעברית ו/או באנגלית בלבד, לכל היבטי אבטחת המידע בפרויקט. לאחר קבלת התיעוד, הספק יהיה אחראי במידת הצורך לשנות ולהוסיף פרטים לתיעוד שהגיש בהתאם לדרישות גופי אבטחת המידע במשטרת ישראל.

1.18.2 התיעוד יכלול את תהליך העבודה המוצע שלב אחרי שלב , ויכלול שרטוטים גראפיים תוך פרוט פתרונות האבטחה המיושמים כחלק מהפתרון הכולל. כמו כן, התיעוד יכלול את כלל רכיבי הפתרון בהן ייעשה שימוש במערכת, בכללותה על כל מרכיביה (לרבות הפלטפורמה).

1.19 <u>דרישות חובה רלוונטיות ייעודיות לענן:</u>

1.19.1 הפרדה מוחלטת בין נתוני חברת הדואר לבין נתונים של לקוחות אחרים הנשמרים בענן.

1.19.2 זיהוי מלא של שימוש וגישה לנתוני חברת הדואר בכל תצורת ענן IaaS, PaaS, SaaS .

1.19.3 הגדרת מדיניות אבטחה:

א. יכולת הגדרת Policy חדש

ב. יכולת יצירת Policy אד הוק

1.19.4 יכולת חיפוש היסטורית בכל שירותי ה- SAAS השונים אחר מרכיבים ופעולות

שבוצעו במסגרת ה –POLICIES שהוגדרו.

1.19.5 תמיכה בריבוי פרופילים.

1.19.6 יכולות גיבוי ושחזור כולל בדיקות תקינות נתונים בשחזורים תקופתיים.

1.19.7 DLP- יכולת מתן גישה ו/או מניעת גישה של מכשירים לא ארגוניים לשירותי הענן הארגונים והכפפת מדיניות DLP עליהם.

1.19.8 Context-Sensitive Analysis – המערכת תקנה יכולת לניתוח תוכן רגיש אחר קבצים נכנסים ויוצאים מסביבת הענן הארגוני.

1.19.9 יכולות זיהוי מלאות עבור UBA (User Behavior Analytics) – זיהוי ניסיונות גישה ופעילות חריגה בהתנהגות המשתמש, חסימת חיבורים וניסיונות גישה ממדינות זרות/עוינות, זיהוי ניסיונות גישה בו זמנית מאזורים שונים, מכשירים שונים וכדומה.

1.19.10 תמיכה בצורה מלאה ב- MFA (Multi-Factor Authentication).

1.19.11 יכולת הצפנה מלאה (In rest + On Transit) של נתונים רגישים, שיוגדרו בהתאם למדיניות חברת הדואר.

1.19.12 אספקת אפשרות ללוגים בפורמט מקובל כגון : SYSLOG

1.19.13 המערכת תספק יכולת קונסולידציה של "לוחות המכוונים" (Dashboards) המבוססים על מנגנוני ההגנה הקיימים בכלל שירותי ה- SAAS הארגונים (Office365,Google Apps, Salesforce וכדומה).

1.19.14 Cross Platform Capabilities – המערכת תאפשר קבלת התראות על קורלציה בין שירותי SAAS שונים.

1.19.15 Security Operations & Forensics – המערכת תספק מנגנון התרעות ותחקור אירועים ויזואלי ונוח אחר אירועים שאירעו.

1.19.16 הגברת מודעות המשתמשים בעת זיהוי שימוש באפליקציה בעלת סיכון.