



# **ניהול סיכוני סייבר בשרשרת אספקה**

**הוראת ניהול תקין לפי סעיף 88 יד(א) לחוק הדואר**

### 1. סמכות פיקוח וביקורת:

בהתאם לסמכותי לפי סעיף 88ד(א) לחוק הדואר, התשמ"ו-1986 ("חוק הדואר"), אני קובע הוראות אלה:

### 2. תחולה;

הוראה זו תחול על חברת דואר ישראל בע"מ בנותנה את השירותים הכספיים לפי הוראות פרק 11 לחוק הדואר ("בנק הדואר" או "הבנק").

### 3. תחילה ועדכונים;

<u>גרסה</u>	<u>פרטים</u>	<u>תאריך תחילה</u>
1	גרסה מקורית	מיום ט"ז באייר ה'תשע"ח, 01 במאי 2018.

### 4. הגדרות;

בהוראה זו-

"גורמי חוץ" -

גורמים הנותנים שירותים לבנק הדואר בתחומים הקשורים לטכנולוגית המידע, כגון: תמיכה ו/או תחזוקת מערכת המידע, אחסון נתונים רגישים מחוץ לחצרי הבנק, שירותי מיקור חוץ טכנולוגיים, וכד';

"וועדת היגוי" -

כהגדרתה בסעיף 2.2.3. להוראת ניהול תקין בנושא "ניהול טכנולוגיות המידע ואבטחת מידע במערכות מידע בנק הדואר";

## 5. מבוא;

**5.1.** בשנים האחרונות גדל מספר אירועי הסייבר המתרחשים בארגונים פיננסיים בעולם ובישראל. אירועים אלו מתאפיינים ברובם, בין היתר, בגרימה של נזק רב ובשיטות תקיפה מתוחכמות וחדשניות, שמקורן לעתים בגורמים חיצוניים המספקים שירותים שונים לתאגידים הפיננסיים. גורמים אלו נכללים בשרשרת האספקה של התאגידים הפיננסיים.

חלק מגורמי החוץ הנכללים בשרשרת האספקה של התאגיד הפיננסי, הינם מהותיים לפעילותו וחושפים אותו לסיכוני סייבר ואבטחת מידע פוטנציאליים גבוהים אשר בהתממשותם ניתן לתקוף את התאגיד הפיננסי או לפגוע בפעילותו.

**5.2.** מטרת הוראה זו הינה להבהיר את האחריות של בנק הדואר בנוגע לקיום סביבת עבודה מאובטחת מול הספקים המהותיים, ואת חובותיו לניהול סיכוני סייבר הולמים בפעילות ספקים אלו בחצרותיהם, בחצרי בנק הדואר ובממשקים שלהם עם בנק הדואר.

## 6. כללי;

**6.1.** בנק הדואר יגדיר מהם הפרמטרים להגדרת ספקים מהותיים בבנק הדואר.

**6.2.** בנק הדואר יקבע עקרונות להתחייבויותיהם של ספקים מהותיים כלפי בנק הדואר בהתייחס לניהול סיכוני סייבר.

**6.3.** בנק הדואר יגדיר בהסכם ההתקשרות עם הספק המהותי התייחסות פרטנית לנושא ניהול סיכוני סייבר ויוודא כי הספק עומד בעקרונות שהגדיר בנק הדואר.

**6.4.** בנק הדואר יערוך אחת לתקופה:

**6.4.1.** מיפוי של הספקים המהותיים של בנק הדואר; בחינה של הסכם ההתקשרות עימם; עמידתם בהתחייבויותיהם החוזיות; זאת, תוך התייחסות לצורך בשינויים הנדרשים מהספק כתוצאה מהתפתחויות ושינויים טכנולוגיים ושינויים בשירותים הניתנים.

**6.4.2.** הערכת סיכונים הנגזרים מהשירותים הניתנים ע"י הספקים המהותיים בהתבסס גם על הבחינה כאמור בסעיף 6.4.1 לעיל ותוצאות הסקרים שבסעיף 7.1.3 להלן.

**6.5.** היה וגורמים רלוונטיים בבנק הדואר יגיעו למסקנה לאחר הבחינה כאמור בסעיף 6.4 לעיל, כי הספק המהותי אינו עומד בהתחייבויותיו, ובאופן שחושף את בנק הדואר לסיכוני סייבר משמעותיים, עליהם לדווח להנהלת בנק הדואר,

תוך הצגת סיכונים אלו והשלכותיהם על בנק הדואר ולקוחותיו. במקרה זה, על ההנהלה יהיה לשקול ולהחליט בדבר המשך ההתקשרות עם הספק.

## 7. הסכם התקשרות;

**7.1.** במסגרת הסכם ההתקשרות של בנק הדואר עם הספק המהותי, בנק הדואר ייקח בחשבון את הצורך בשילוב ההיבטים הבאים בהסכם, בהתאם להערכת הסיכונים:

- 7.1.1.** הקשחת מערכות הספק המהותי המותקנות ברשת בנק הדואר בהתאמה לנהלי אבטחת המידע וניהול הסיכונים של בנק הדואר.
- 7.1.2.** העברת קבצי Log ממערכות הספק, לפי בקשת בנק הדואר.
- 7.1.3.** עריכת סקר פגיעויות ומבדקי חדירה מבוקרים אחת לתקופה לפי דרישת בנק הדואר.
- 7.1.4.** טיפול בממצאים שזוהו בסקר ובמבדקי החדירה תוך פרק זמן סביר לאחר גילויים.
- 7.1.5.** ביצוע בדיקת מהימנות לעובדי הספק המהותי הקשורים לשירות הניתן לבנק הדואר.
- 7.1.6.** הצגת רשימה של ספקי משנה אשר תומכים בשירותים הניתנים לבנק הדואר ע"י הספק המהותי מידי תקופה שתיקבע ע"י בנק הדואר.
- 7.1.7.** קביעת הסדרים למחיקת נתונים של בנק הדואר המאוחסנים בחצרי הספק, לאחר סיום ההתקשרות או לפי דרישת בנק הדואר.
- 7.1.8.** ביצוע הפרדה בחצרי הספק המהותי בין סביבת העבודה (פיתוח, ייצור, וכד').
- 7.1.9.** דיווח לבנק הדואר על אירועי סייבר אשר יתרחשו אצל הספק המהותי או אצל ספקי משנה שלו.
- 7.1.10.** הפסקת ההתקשרות מצד בנק הדואר עם הספק המהותי בעת שהופרו תנאים מתנאי ההסכם על ידי הספק המהותי.

## 8. תמיכה ותחזוקה;

**8.1.** בנק הדואר יגדיר פעילויות בהתאם להערכת הסיכונים, עבור נדרש הספק המהותי לאמצעי זיהוי חזקים (2-Factor Authentication) בפעילויות, כגון: גישה מרחוק למערכות בנק הדואר, פעילות תחזוקה במערכות בנק הדואר, וכד'.

**8.2.** בנק הדואר יקבע מנגנוני אבטחה ובקרה בגישה מרחוק של הספק המהותי, בהתאם להערכת הסיכונים, כגון: מניעת גישה אלא אם אושרה על ידו; גישה מאובטחת ומסביבת פעילות נפרדת מיתר סביבות העבודה של הספק המהותי; הפעלת מנגנון ניתוק התקשורת לאחר פרק זמן שבו לא בוצעה פעילות מצד הספק המהותי; הקלטת וניטור פעילות תחזוקה; וכד'.

**9. פיקוח ומעקב;**

**9.1.** מנהל אבטחת המידע בבנק הדואר יהיה האחראי על יישום האמור בהוראה זו. ככל שימצא חריגה מהוראה זו ידווח על כך מיידית לוועדת ההיגוי.

**9.2.** הנהלת בנק הדואר תוודא כי למנהל אבטחת המידע יש את הכלים והמשאבים לצורך קיום האמור בהוראה זו.

**10. בקרה ודיווחים;**

**10.1.** אחת לרבעון ידווח מנהל אבטחת המידע לוועדת ההיגוי על התפתחויות בסיכוני הסייבר בשרשרת האספקה. ועדת ההיגוי תעביר דיווחים בנושא ניהול סיכוני הסייבר להנהלת בנק הדואר אחת לשנה לכל הפחות, לרבות בנוגע לאמור בסעיפים 6 ו-9 בהוראה זו ובפרט בנוגע לסעיפים 6.4 ו-6.5.

\* \* \*