

**משרד התקשורת
אגף פיקוח בנק הדואר**



**הוראת ניהול תקין על פי הוראות סעיף
88 לחוק הדואר, התשמ"ו-1986**

**ניהול טכנולוגיות המידע
ואבטחת מידע במערכות המידע**

- בנק הדואר -

1. מבוא..... 3

1.1 סמכות 3

1.2 מטרת ההוראה 3

1.3 הגדרות ומונחים 4

2. ממשל טכנולוגיות מידע..... 7

2.1 יעדים 7

2.2 סמכות ואחריות של גורמי הניהול 7

2.3 ניהול השקעות בתחום טכנולוגיות המידע..... 12

2.4 הפרדת מערכות המידע המשמשות את בנק הדואר; 14

3. ניהול סיכוני טכנולוגיות מידע..... 15

3.1 יעדים 15

3.2 קווים מנחים 15

3.3 גיבוש תהליך 15

3.4 ניהול שוטף 16

3.5 דיווח 17

4. ניהול מידע..... 18

4.1 ניהול נכסי טכנולוגיות מידע..... 18

4.2 ניהול שינויים 20

4.3 גיבוי ושחזור נתונים 22

5. תפעול מערך אבטחת מידע..... 24

5.1 אבטחה פיזית וסביבתית..... 24

5.2 ניהול תקשורת ותפעול..... 25

5.3 בקרת גישה 27

6. רציפות במתן שירותים..... 29

6.1 יעדים 29

6.2 קווים מנחים 29

6.3 גיבוש תהליך 30

6.4 ניהול שוטף 31

6.5 דיווח 32

7. מיקור חוץ..... 33

7.1 יעדים 33

7.2 קווים מנחים 33

7.3 גיבוש תהליך 33

7.4 ניהול שוטף 34

7.5 דיווח 34

8. אספקת שירותים בתקשורת..... 35

8.1 יעד 35

8.2 קווים מנחים 35

8.3 גיבוש תהליך 35

8.4 ניהול שוטף 36

8.5 דיווח 36

9. פרק ט': החלת ההוראה..... 38

9.1 תחולה 38

9.2 תחילה 38

1. מבוא;

1.1. סמכות;

בהתאם להוראות סעיף 88ד(א) לחוק הדואר, התשמ"ו-1986 ("החוק" או "חוק הדואר") מצ"ב הוראת ניהול תקין לחברת דואר ישראל בע"מ ("החברה" או "חברת הדואר") בנונתה את השירותים הכספיים לפי סעיף 88א לחוק הדואר, התשמ"ו-1986 ("בנק הדואר" או "הבנק"), בנושא ניהול טכנולוגיות המידע ואבטחת מידע במערכות מידע בבנק הדואר ("הוראה").

1.2. מטרת ההוראה;

מערך טכנולוגיית המידע ואבטחת המידע במערכות המידע של בנק הדואר, מהווה מרכיב מרכזי בתפעול ובניהול בנק הדואר. על כן, נדרשים דירקטוריון החברה, והנהלת הבנק לגבש תהליכי עבודה בתחום, להגדיר את הסמכות והאחריות של בעלי תפקידים בהיררכיה הניהולית, להקצות את המשאבים הנחוצים ולנטר את הפעילויות השונות, במטרה להבטיח את ניהולם התקין של מערכי טכנולוגיות המידע ואבטחת המידע בכל הנוגע לשירותים הכספיים, תוך תמיכה בפעילות העסקית של הבנק, ושמירה על החיסיון (סודיות), השלמות והזמינות של נכסי המידע שלו.

הוראה זו נכתבה במטרה להתאים לאופי ופעילות בנק הדואר והיא מושתתת על מתודולוגיות וסטנדרטים מקובלים לממשל טכנולוגיות המידע ולניהול אבטחת המידע, וכן על חוקים ורגולציות הקיימים בישראל, כמפורט:

- 1.2.1 CobiT 4.1 - מסגרת בקרה מקובלת לעניין קיום ענייני בקרה ופיקוח יעילים בתחום טכנולוגיות המידע;
- 1.2.2 ISO 27001 - תקן בינלאומי לאבטחת מידע;
- 1.2.3 BS 25999 - תקן בריטי להמשכיות עסקית;
- 1.2.4 SSAE16/SAS70 - תקן של AICPA בנושא עקרונות נאותים של בקרה פנימית;
- 1.2.5 הוראה לניהול בנקאי תקין, ניהול טכנולוגיות המידע, הוראה 357 של המפקח על הבנקים;
- 1.2.6 הוראה לניהול סיכונים אבטחת המידע של הגופים המוסדיים, חוזר מספר 2006-9-6 משרד האוצר, אגף שוק ההון, ביטוח וחסכון;
- 1.2.7 הוראה לניהול טכנולוגיות מידע בגופים מוסדיים, חוזר מספר 2010-9-04 משרד האוצר, אגף שוק ההון, ביטוח וחסכון;
- 1.2.8 הוראה לניהול בנקאי תקין, ניהול המשכיות עסקית, הוראה 355 של המפקח על הבנקים;
- 1.2.9 הוראה לניהול בנקאי תקין, ניהול סיכון תפעולי, הוראה 350 של המפקח על הבנקים;
- 1.2.10 רישיון כללי לחברת דואר ישראל בע"מ למתן שירותי דואר, שירותים כספיים מטעם החברה הבת ושירותים נוספים, ("הרישיון");
- 1.2.11 חוק הדואר;

- 1.2.12. תקנות הדואר (שירותי דואר בסיסים ושירותים כספיים אשר יינתנו לכלל הציבור בכל המדינה), תשס"ח - 2008, ("תקנות שירותים כספיים בסיסיים").
- 1.2.13. צו איסור הלבנת הון (חובות זיהוי, דיווח וניהול רישומים של בנק הדואר למניעת הלבנת הון ומימון טרור), התשע"א - 2010, ("צו איסור הלבנת הון").
- 1.2.14. חוק הביקורת הפנימית, תשנ"ב - 1992;
- 1.2.15. חוק הגנת הפרטיות התשמ"א - 1981, ("חוק הגנת הפרטיות");
- 1.2.16. תקנות הגנת הפרטיות (תנאי החזקת מידע ושמירתו וסדרי העברת מידע בין גופים ציבוריים), התשמ"ו - 1986;
- 1.2.17. תקנות והנחיות ארכיון המדינה לביעור ולשמירה של מסמכים.

1.3. הגדרות ומונחים;

להלן הגדרות ומונחים בהן נשתמש בהוראה, כמפורט:

כללי

- 1.3.1. שירותים כספיים - כהגדרתם בסעיף 1 לחוק הדואר;

ניהול השקעות בתחום טכנולוגיות המידע

- 1.3.2. סל שירותי טכנולוגיות המידע (IT Portfolio) - לרבות סל שירותי אבטחת מידע במערכות המידע; מגדיר את סט השירותים שמספק אגף מערכות המידע, אשר נבחנו ונמצאו כתומכים ביעדים העסקיים של הארגון.

ניהול נכסי טכנולוגיות מידע

- 1.3.3. ניהול טכנולוגיות המידע - מכלול הפעילויות, הנדרשות לשם ניהול יעיל, מועיל ותקין של מערכות המידע לרבות אבטחת מידע במערכות המידע, תוך מזעור הסיכונים השונים והקניית תועלת עסקית ממשית לבנק הדואר.
- 1.3.4. נכס מידע - נתונים המאוחסנים באופן אלקטרוני (לדוגמה מאגר נתונים) או במסמכי נייר.
- 1.3.5. נכס טכנולוגיות המידע - מערכת מידע או רכיביה לדוגמה חומרה, תוכנה ומערכת הפעלה.
- 1.3.6. סיווג - קטלוג של נכסי מידע, על פי מידת החיסיון הנדרשת עבורם ובהתאם למדרג אשר הוגדר מראש.
- 1.3.7. מערכת ליבה - מערכת מידע בעלת השפעה מהותית על שירותי הבנק.
- 1.3.8. בעל מידע - גורם מהתחום העסקי, האמון על נכס מידע, ובין היתר, אחראי על סיווג הנכס, ואישור הרשאות גישה אליו.
- 1.3.9. נאמן המידע - אחראי להבטיח את קיומם התקין של תהליכי עבודה, לרבות גיבויים, שחזורים יזומים והקצאת הרשאות, על פי הנחיות בעל המידע ובהתאם לנוהג מיטבי בתחום.
- 1.3.10. מידע רגיש - מידע שהוגדר כסודי מהיבטי בטחון המדינה, מידע מוגבל לפי חוק הגנת הפרטיות, או מידע שהוגדר כרגיש ע"י הנהלת הבנק.

ניהול שינויים

- 1.3.11. שינויים** - שינויים בנכסי המידע ובנכסי טכנולוגיית המידע, הנדרשים בין היתר כתוצאה משינוי בתהליך עסקי, שיפור תהליך עסקי או שינויים טכנולוגיים.
- 1.3.12. שינויי חירום** - שינויים בנכסי המידע ובנכסי טכנולוגיית המידע הנדרשים באופן מיידי, בדרך כלל כתוצאה מתקלה או ליקוי מהותי, ואשר לא ניתן לבצעם בהתאם לסדר הפעולות המיטבי, בתהליך ניהול שינויים.

גיבוי ושחזור נתונים

- 1.3.13. מחזוריות תהליך הגיבוי** - קובעת את תדירות ביצוע הגיבוי, סוג הגיבוי, ופרק זמן מינימאלי לשמירת מצע הגיבוי, עד הכנסתו מחדש לסבב הגיבויים.
- 1.3.14. Off-site** - אתר לאחסון מצעי גיבוי, מחוץ לחצרי הבנק, במטרה להגן על מצעי הגיבוי בפני מקרי קיצון במתחם הבנק.

ניהול תקשורת ותפעול

- 1.3.15. נתיב בקרה** - תיעוד פעולות המתבצעות במערכות מידע. קובץ התיעוד מקשר בין הפעולה לנתונים נוספים כגון: שם מבצע הפעולה, מועד הביצוע, מהות הפעולה ועוד.
- 1.3.16. הצפנה** - יישום הממיר מידע גלוי (Clear text) למידע מקודד (Cipher text) באופן שיוכל להיות מפוענח אך ורק לגורמים מורשים.
- 1.3.17. מערכת סינון תוכן (Content Filtering)** - רכיב טכנולוגי המאפשר לסנן, בהתאם לסיכונים ולמדיניות הבנק, תכנים מרשתות חיצוניות, בעלי אופי פוגעני, או בעלי אופי לא עסקי.
- 1.3.18. חומת אש (Firewall)** - רכיב טכנולוגי, היוצר חיץ בין רשתות הבנק לרשתות חיצוניות ומבקר את התעבורה הנכנסת ויוצאת מרשתות הבנק, בהתאם למדיניות אבטחה מוגדרת.
- 1.3.19. מערכת מניעת חדירה (Intrusion Prevention System) - IPS** - רכיב טכנולוגי, המנתח תעבורת נתונים ברשת התקשורת. רכיב זה מזהה, מתריע וחוסם תעבורה לא לגיטימית וניסיונות תקיפה, בהתאם למדיניות אבטחה מוגדרת.

בקרת גישה

- 1.3.20. אמצעי זיהוי** - אמצעי המספק אימות לגבי זהותו של אדם, דוגמת שם חשבון משתמש או כרטיס חכם, בתהליך ההזדהות והכניסה למערכות מידע.

רציפות במתן השירותים

- 1.3.21. תוכנית המשכיות עסקית (Business Continuity Plan) - BCP** - תוכנית אשר נועדה לאפשר המשך מתן שירותים רציף, בעקבות מקרה אסון רחב היקף.
- 1.3.22. תהליך ניתוח השלכות עסקיות (Business Impact Analysis) - BIA** - תהליך המשמש להערכת ההשפעה על פעילות הבנק והמוניטין שלו, כתוצאה מהתממשות סיכונים פוטנציאליים על שירותי הבנק.

1.3.23. תוכנית התאוששות טכנולוגית (DRP (Disaster Recovery Plan) - מהווה חלק מתוכנית ההמשכיות העסקית. תוכנית זו מתמקדת בהשבת המערכות הטכנולוגיות לפעילות תקינה.

1.3.24. שיגרת חרום - פרק הזמן החולף בין הפעלת השירותים העסקיים באתר החרום בעקבות אסון, לבין החזרה לשגרה, באתר הייצור של הבנק.

1.3.25. RLO (Recovery Level Objective) - רמת השירות בו יופעלו שירותי הבנק בשגרת חרום. פרמטר זה מגדיר את רמת השירות המסופקת בשגרת חרום, כאחוז מרמת השירות הניתן על ידי הבנק בשגרה.

1.3.26. RTO (Recovery Time Objective) - פרק הזמן המרבי, הנדרש להשבת שירות של הבנק שכשל או הושבת, לרמת השירות אשר הוגדרה עבורו בשגרת חרום (RLO), לרבות פרק הזמן הנדרש לאישוש המערכת הטכנולוגית.

1.3.27. RPO (Recovery Point Objective) - הנקודה בזמן, אליה יאוחזר המידע בעקבות אסון. פרמטר זה מגדיר את כמות המידע שהארגון מוכן לאבד בעקבות אסון, במונחי שעות עבודה.

1.3.28. פרק זמן מקסימאלי להפרעה ברמת שירות – MTPOD (Maximum Tolerable Period of Disruption) - פרק הזמן המקסימאלי במהלך שיגרת החרום, במהלכו ניתן לספק שירות של הבנק, ב-RLO אשר הוגדר עבורו, ללא פגיעה מהותית בתפקוד הבנק.

מיקור חוץ

1.3.29. הסכם רמת שירות (SLA (Service Level Agreement) - הגדרה ברורה וברת מדידה של רמת שירות, המתייחסת בין היתר לזמן תגובה ולחלון השירות - הימים ושעות העבודה, במסגרתן יינתן השירות.

1.3.30. הסכם רמת תפעול (OLA (Operational Level Agreement) - הגדרה ברורה וברת מדידה של היקף השירות המסופק, לרבות מידת הזמינות של נכסי טכנולוגיות המידע, התומכים בתהליכים עסקיים.

1.3.31. SAS70 - תקן של ה- (American Institute of Certified Public Accountants) **AICPA** - העוסק בנושאי ביקורת חשבונאית, ביקורת מערכות מידע וביקורת פנימית, על נותני שירותים במיקור חוץ. תקן **SAS70** מעניק ללקוחות ולמבקרים את הביטחון, כי נותן שרות העונה לדרישות התקן, מיישם עקרונות נאותים של בקרה פנימית. תקן **SAS70** הוחלף בשנת 2011 בתקן **SSAE16**.

2. ממשל טכנולוגיות מידע;

2.1. יעדים;

הקמת מסגרת אפקטיבית של ממשל טכנולוגיות מידע ואבטחת מידע כחלק מממשל תאגידי, לרבות הגדרת מבנה ארגוני, תהליכים, תפקידים ואחריות, על מנת לוודא ניהול תקין של תחום טכנולוגיות המידע ואבטחת מידע אשר יתמוך ביעדים ובשירותים של בנק הדואר. מטרת יישום ממשל טכנולוגיות מידע ואבטחת מידע בבנק הדואר, הינן הגדרת קווים מנחים וכן ביצוע פעולות פיקוח, ניטור ובקרה שוטפות, על מנת להבטיח כי כלל הפעילויות וההשקעות בתחום טכנולוגיות המידע ואבטחת המידע, יתאימו למדיניות הבנק וליעדיו העסקיים, לרבות עמידה בדרישות כל דין והרגולציה.

2.2. סמכות ואחריות של גורמי הניהול;

2.2.1. סמכות ואחריות דירקטוריון חברת הדואר;

לאור חשיבותו של מערך טכנולוגיות המידע ואבטחת המידע לפעילות העסקית של הבנק וכן לאור היקף התקציב המוקצה לתחום זה, נדרש דירקטוריון החברה להקים, להתוות, להנחות ולקיים מנגנון לפיקוח-על, על תחום טכנולוגיות המידע ואבטחת המידע. לשם כך יעסוק הדירקטוריון, בין היתר, בתחומים הבאים:

2.2.1.1. גיבוש אסטרטגיה לתחום טכנולוגיות המידע ואבטחת מידע, הנגזרת

מהאסטרטגיה העסקית של בנק הדואר בכל הנוגע לשירותים הכספיים;

2.2.1.2. אישור מדיניות בתחום טכנולוגיות המידע ואבטחת מידע בכל הנוגע לשירותים הכספיים, אשר תתייחס, בין היתר, לכל אחד מהתחומים הבאים:

א. ניהול נכסי מידע ונכסי טכנולוגיות המידע, בהתאם לדרישות פרק 4 להלן;

ב. ניהול סיכונים, בהתאם לדרישות פרק 3 להלן;

ג. מסגרת עבודה בתחום רציפות מתן שירותים כספיים בבנק הדואר (המשכיות עסקית), בהתאם לדרישות פרק 6 להלן;

ד. מיקור חוץ, בהתאם לדרישות פרק 7 להלן;

ה. המדיניות תכלול, בין היתר, תפיסה, מטרות, יעדים, דרכים, אמצעים, תפקידים ותחומי אחריות, קווים מנחים, גישות ציות לכל דין ולרגולציה והפניה לנהלים.

2.2.1.3. התוכנית האסטרטגית ומדיניות בנק הדואר בנוגע לשירותים הכספיים

יסקרו ויבחנו לפחות אחת לשנה, ויעודכנו, בהתאם לשינויים בסביבה העסקית, במפת הסיכונים ובדרישות כל דין ורגולציה;

- 2.2.1.4.** אישור תכנית העבודה השנתית והרב-שנתית בתחום טכנולוגיות המידע ואבטחת מידע בכל הנוגע לשירותים הכספיים;
- 2.2.1.5.** יישום מנגנוני פיקוח, ניטור ובקרה נאותים על פעילות הבנק בתחום טכנולוגיות המידע ואבטחת מידע, לרבות ביצוע פיקוח ומעקב אחר פרויקטים מרכזיים ושינויים מהותיים, במערכות הליבה של הבנק;
- 2.2.1.6.** הבטחת יישומם של מנגנוני אכיפה אפקטיביים פנימיים בבנק, על מנת להבטיח את עמידת הבנק בדרישות הציות החיצוניות והפנימיות בתחום טכנולוגיות המידע ואבטחת מידע במערכות מידע;
- 2.2.1.7.** הגדרת מודל דיווח לדירקטוריון, בתחום טכנולוגיות המידע ואבטחת מידע במערכות מידע, אשר יגדיר בין היתר, את הגורמים האחראיים לדווח, נושאי הדיווח ותדירות הדיווח;
- 2.2.1.8.** קיום דיון בנושא טכנולוגיות המידע ואבטחת מידע במערכות מידע, לפחות אחת לשנה וכן לפני ביצוע שינויים מהותיים במערך טכנולוגיות המידע או אבטחת מידע במערכות מידע או בעקבות אירועים חריגים.

2.2.2. סמכות ואחריות הנהלת בנק הדואר ;

על הנהלת בנק הדואר, חלה החובה להבטיח את ניהולו התקין של תחום טכנולוגיות המידע ואבטחת המידע במערכות מידע באופן המוודא שימוש יעיל, אפקטיבי והולם בטכנולוגיות המידע, התואם ליעדים, למדיניות ולצרכי הבנק ותומך בהשגתם. במסגרת זו על הנהלת בנק הדואר לפעול לביצועם של לפחות כל אחד מאלה:

- 2.2.2.1.** גיבוש ותחזוקה של מדיניות טכנולוגיות מידע ואבטחת מידע במערכות המידע, אשר תתמוך באסטרטגיה כאמור בסעיפים 2.2.1.1 ו-2.2.1.2 לעיל.
- 2.2.2.2.** אישור מסגרת הנהלים, כנדרש בסעיף 2.2.4.5 להלן.
- 2.2.2.3.** מינוי אחד מחברי ההנהלה כממונה אבטחת מידע, אשר יהיה אמון על יישומן של המדיניות ותוכניות העבודה של הבנק, בתחום אבטחת המידע;
- 2.2.2.4.** גיבוש תכנית עבודה שנתית ותכנית עבודה רב-שנתית, בתחום טכנולוגיות המידע ואבטחת מידע במערכות המידע, וביצוע פיקוח, ניטור ובקרה שוטף אחר ביצוען;
- 2.2.2.5.** התאמת תוכנית העבודה של תחום טכנולוגיות המידע ואבטחת מידע במערכות המידע ליעדי בנק הדואר ולתכניות העבודה של היחידות העסקיות שלו. במסגרת זו על הנהלת הבנק להבטיח תאימות של המשאבים המוקצים לתחום טכנולוגיות המידע ואבטחת מידע במערכות המידע, לרבות התאמת התקציב השוטף, תקציבי ההצטיידות וההשקעות בתחום זה.

- 2.2.2.6.** יישום תהליכים סדורים אשר יבטיחו ציות לחוקים ורגולציות המשפיעים על תחום טכנולוגיות המידע ואבטחת המידע במערכות המידע. בין היתר, יש למנות גורם אחראי אשר ירכז את הנושא, וידווח לדירקטוריון, לכל הפחות אחת לשנה, על מידת העמידה בדרישות אלו.
- 2.2.2.7.** הגדרת מדדי ביצוע לרבות רמות שירות (SLA) ורמות תפעול (OLA) מוגדרות מול המשתמשים הפנימיים, שותפים עסקיים, ספקים ולקוחות הבנק;
- 2.2.2.8.** הגדרת מודל דיווח להנהלה, בתחום טכנולוגיות המידע ואבטחת מידע במערכות המידע, אשר יגדיר בין היתר, נושאי דיווח לרבות עמידה במדדים, תדירות הדיווח וכן דיווח בעקבות אירועים חריגים;
- 2.2.2.9.** יישומה ותחזוקתה של תוכנית המשכיות עסקית בכל הנוגע לשירותים הכספיים, כאמור בפרק 6.

2.2.3. ועדת היגוי;

- על הנהלת בנק הדואר, למנות ועדת היגוי מקצועית בראשות מנהל הבנק, אשר תעסוק בתחום טכנולוגיות המידע ואבטחת מידע ("ועדת היגוי"). בין חבריה הקבועים יכללו גורמים עסקיים בכירים, וכן, סגן מנהל בנק הדואר למערכות המידע, ומנהל אבטחת מידע של הבנק.
- על הנהלת הבנק לגבש כתב מינוי לוועדת ההיגוי, אשר יגדיר את תפקידיה, סמכויותיה ואחריותה של ועדת ההיגוי, יגדיר את החברים בה ויקבע את מועדי התכנסותה ובלבד שלא יפחתו מאחת לרבעון.
- ועדת ההיגוי תעסוק, לכול הפחות, בתחומים הבאים:
- 2.2.3.1.** הובלת פעילות הבנק, בכל הקשור לניהול התקין של תחום טכנולוגיות המידע ואבטחת המידע במערכות המידע בהתאם למדיניות דירקטוריון החברה.
- 2.2.3.2.** תיעדוף וביצוע מעקב אחר יישום תכניות העבודה ופרויקטים מהותיים בתחום, בהתאם למדיניות דירקטוריון החברה והנחיות הנהלת הבנק.
- 2.2.3.3.** דיווח לדירקטוריון, לפחות אחת לחצי שנה, על נושאים מרכזיים המצויים בטיפול.

2.2.4. תפקיד מנהל מערכות המידע;

- הנהלת בנק הדואר תמנה מנהל מערכות מידע לבנק, אשר יהיה אחראי על כלל הפעילויות בתחום טכנולוגיות המידע, ויהיה במעמד חבר הנהלת הבנק או יהיה כפוף ישירות למנהל הבנק ("מנהל מערכות מידע").
- במסגרת תפקידו, עליו לבצע בין היתר, את הפעולות הבאות:

- 2.2.4.1.** ניהול אגף מערכות המידע של הבנק, גיבוש המבנה הארגוני שלו ואבטחת הרמה המקצועית הנדרשת, כדי להקים, לתחזק, לתמוך ולפתח את מערכות המידע של הבנק;
- 2.2.4.2.** ביצוע תוכנית העבודה השנתית והרב-שנתית, כפי שגובשה על ידי הנהלת הבנק ואושרה על ידי דירקטוריון החברה;
- 2.2.4.3.** גיבוש תהליכי עבודה נאותים בתחום טכנולוגיות המידע, התואמים את צרכי הבנק ועונים על דרישות החוק והרגולציה, אליהם כפוף הבנק;
- 2.2.4.4.** תמיכה בצורכי המשתמשים ובתשתיות הטכנולוגיות של הבנק ועמידה ברמות שירות (SLA) וברמות תפעול (OLA), בהתאם לדרישות סעיף 2.2.2.7;
- 2.2.4.5.** יישום מסגרת נהלים מתאימה בתחום ניהול טכנולוגיות המידע ואבטחת המידע במערכות המידע. לכל הפחות, ייכתבו נהלים לכל הנושאים המפורטים בהוראה זו;
- 2.2.4.6.** עדכון נהלים באופן שוטף בהתאם לשינויים החלים בסביבה העסקית ובסביבה הטכנולוגית, ולכל הפחות אחת ל-18 חודש;
- 2.2.4.7.** יישום תכניות הדרכה למשתמשים הכוללות התייחסות להטמעת מערכות חדשות, לשימור הרמה המקצועית ולעדכון שוטף של משתמשי המערכות.
- 2.2.4.8.** מנהל מערכות מידע לא ישמש בתפקיד מנהל אבטחת מידע בבנק.
- 2.2.5. סמכות ואחריות מנהל אבטחת המידע של בנק הדואר;**
- הנהלת בנק הדואר תמנה מנהל אבטחת מידע לבנק, בעל כישורים וניסיון בתחום אבטחת מידע, אשר יהיה כפוף מקצועית לממונה אבטחת מידע של בנק הדואר. במסגרת תפקידו, יהיה מנהל אבטחת המידע אחראי על יישומה בפועל של מדיניות אבטחת המידע בכל הנוגע לשירותים הכספיים ויעסוק, בין היתר, בתחומים הבאים:
- 2.2.5.1.** בקרה על תהליכים שונים בבנק הדואר, בהיבטי אבטחת מידע;
- 2.2.5.2.** אחריות על הטמעה של נהלי אבטחת מידע, וליווי תהליך היישום של פתרונות אבטחת מידע;
- 2.2.5.3.** הנחייה מקצועית של הבנק, בנושאי אבטחת מידע;
- 2.2.5.4.** יישום מערך הדרכות בנושא אבטחת מידע.
- מנהל אבטחת המידע לא יעסוק בתפקידים ביצועיים ותפעוליים אשר עלולים לגרום לניגוד עניינים.
- 2.2.6. סמכות ואחריות מנהל סיכוני טכנולוגיות מידע;**
- הנהלת בנק הדואר תמנה למטה בנק הדואר מנהל סיכוני טכנולוגיות מידע ("מנהל סיכונים"), אשר יהיה אחראי לתיאום הפעילויות של כלל היחידות הקשורות למסגרת ניהול סיכוני טכנולוגיות מידע ואבטחת מידע הטבועים בפעילויות הבנק.
- 2.2.6.1.** מנהל הסיכונים יהיה בעל הכישורים מתאימים לביצוע תפקידו.

- 2.2.6.2** מנהל הסיכונים יהיה בלתי תלוי ולא יקבל החלטות עסקיות הכרוכות בנטילת סיכונים עליהם הוא מפקח;
- 2.2.6.3** מנהל הסיכונים יהיה כפוף למנהל הבנק;
- 2.2.6.4** במסגרת תפקידו, יבטיח מנהל סיכוני טכנולוגיות מידע פיקוח נאות, על אופן ניהול סיכונים אלה בפעילות הבנק, כאמור בפרק 3. בין היתר, יפעל ליישום התהליכים הבאים:
- א.** קביעת מסגרת עבודה לניהול סיכוני טכנולוגיות מידע ואבטחת מידע במערכות המידע;
- ב.** מעקב אחר יישום המטלות הכלולות בתוכנית ניהול סיכוני טכנולוגיות מידע ואבטחת מידע במערכות מידע;
- ג.** זיהוי וניתוח סיכוני טכנולוגיות מידע לרבות סיכוני אבטחת מידע במערכות מידע בפעילות קיימת וחדשה, לרבות לעניין עסקאות המבוצעות במערכות מידע שלא פנים אל מול פנים (עסקאות מרחוק).
- ד.** קביעת מנגנוני פיקוח, בקרה וניטור שוטפים, לניהול סיכוני טכנולוגיות מידע ואיתור חולשות בבקרה.
- 2.2.7 תפקידי הביקורת הפנימית בתחום טכנולוגיות המידע ואבטחת מידע במערכות המידע בכל הנוגע לפעילות הבנק;**
- 2.2.7.1** כחלק מאחריותה הכוללת, תבצע הביקורת הפנימית של חברת הדואר, ביקורות בנושאי טכנולוגיות המידע ואבטחת מידע במערכות המידע של בנק הדואר.
- 2.2.7.2** הביקורות יבוצעו על ידי אנשי מקצוע בעלי כישורים מתאימים לתחום טכנולוגיות המידע ואבטחת המידע.
- 2.2.7.3** פעילות הביקורת תבוצע בהתאם לתוכנית ביקורת אשר תאושר על ידי ועדת הביקורת של חברת הדואר. לכל הפחות, יתקיימו שתי ביקורות בשנה, בתחום טכנולוגיות המידע ואבטחת המידע.
- 2.2.7.4** מסגרת העבודה ותוכנית המשכיות עסקית וכן ממצאי התרגולים בנושא, יסקרו באופן תקופתי על ידי מערך הביקורת הפנימית.

2.3. ניהול השקעות בתחום טכנולוגיות המידע ואבטחת מידע במערכות מידע;

2.3.1. יעדים;

- א. מימוש האסטרטגיה בתחום טכנולוגיות המידע ואבטחת מידע במערכות המידע, כך שפעילויות אגף מערכות מידע ואבטחת מידע, יתמכו ביעדי הבנק;
- ב. שיתוף פעולה בין הגופים העסקיים לבין אגף מערכות מידע ואבטחת מידע של הבנק, כדי לוודא הקצאה אופטימאלית של משאבי טכנולוגיות המידע, לקידום ותמיכה בפעילויות הבנק.
- ג. גיבוש סל שירותי טכנולוגיות המידע, אשר יבטיח בין היתר:
- ג.1. הלימת השירותים הכלולים בו, ליעדים העסקיים של הבנק;
 - ג.2. עמידה ברמת הסיכון המקובלת בבנק בהתאם למדיניות דירקטוריון החברה והנהלת הבנק;
 - ג.3. כי היקף ההשקעות המתוכננות, תואם את התועלת העסקית הצפויה, ואת היקפי הפעילות של הבנק;
 - ג.4. הבטחת יכולת מתן שירותים כספיים בסיסיים;
- ד. גיבוש מדדי הצלחה לאמידת התועלת העסקית.

2.3.2. קווים מנחים;

- 2.3.2.1. באחריות הדירקטוריון, להבטיח את קיומו של תהליך סדור, המבטיח כי שירותים ופרויקטים אשר ישולבו בסל שירותי טכנולוגיות המידע, יתמכו ביעדיו העסקיים של הבנק.
- 2.3.2.2. הדירקטוריון יגדיר מדדים להערכת תרומתם ומידת תמיכתם של שירותים ופרויקטים בתחום טכנולוגיות המידע ואבטחת מידע במערכות מידע, ביעדי הבנק.
- 2.3.2.3. הדירקטוריון יגדיר מנגנוני דיווח, אשר יאפשרו לו לנטר ולבקר פעילויות מרכזיות, הכלולות בסל שירותי טכנולוגיות המידע, על מנת לוודא כי הן עומדות בהיקף המשאבים ומסגרת הזמן אשר הוקצו לביצוען, וכי הן מניבות תרומה משמעותית ליעדים העסקיים של הבנק.
- 2.3.2.4. מעת לעת, יוודא הדירקטוריון כי סל שירותי טכנולוגיות המידע ואבטחת המידע במערכות המידע הינו עדכני ותואם את צרכי הבנק המשתנים.

2.3.3 יישום התהליך;

- 2.3.3.1** הנהלת בנק הדואר תגבש תהליכי עבודה, אשר יאפשרו בין היתר:
- א. תיעודף משימות וגזירת תוכנית עבודה שנתית, מתוך סל שירותי טכנולוגיות המידע ואבטחת המידע במערכות המידע;
 - ב. תקצוב תוכנית העבודה;
 - ג. מעקב אחר יישום תוכנית העבודה, עמידה במסגרת התקציב ולוחות הזמנים שהוגדרו עבור הפעילויות השונות.

- 2.3.3.2** הנהלת בנק הדואר תגבש מודל, המגדיר תחומי סמכות ואחריות של הגורמים השונים המעורבים בניהול פרויקטים מהותיים בנוגע לשירותים הכספיים, לרבות: מנהל בכיר המייצג את לקוחות הפרויקט ואמון על סיומו המוצלח, ועדת ההיגוי ומנהל פרויקט.

2.3.4 ניהול שוטף;

- 2.3.4.1** אחת לשנה, תגבש הנהלת בנק הדואר תוכנית עבודה ומסגרת תקציב, לניהול השקעות ותפעול שוטף של טכנולוגיית המידע ואבטחת המידע במערכות המידע בבנק.
- 2.3.4.2** אחת לרבעון, תבחן הנהלת הבנק, את העלויות בפועל לעומת מסגרת התקציב שהוגדרה.
- 2.3.4.3** על הנהלת הבנק לזהות ולהעריך סטיות ממסגרת התקציב שהוגדרה, ולנקוט בפעולות מתקנות.
- 2.3.4.4** בעזרת מדדים, אשר הוגדרו על ידי הדירקטוריון, תבחן ההנהלה את מידת תרומתן של ההשקעות אשר בוצעו, ליעדים העסקיים של הבנק.

2.3.5 דיווח;

- 2.3.5.1** אחת לרבעון, ידווח מנהל מערכות המידע של הבנק להנהלת הבנק על התקדמות ביישום פרויקטים ושירותים, הכלולים בסל שירותי טכנולוגיות המידע.
- 2.3.5.2** פעמיים בשנה, תדווח הנהלת הבנק לדירקטוריון, אודות תהליך יישומם של פרויקטים ושירותים מהותיים, הכלולים בסל שירותי טכנולוגיות המידע.

2.4. הפרדת מערכות המידע המשמשות את בנק הדואר;

2.4.1. קווים מנחים;

מערכות המידע המשמשות את בנק הדואר יופרדו מיתר מערכות המידע המשמות את חברת הדואר.

2.4.2. ניהול שוטף;

מערכות המידע המשמשות את בנק הדואר ינהלו ויתופעלו בנפרד ממערכות המידע המשמשות את חברת הדואר לצורך פעילותה שאינה קשורה לשירותי בנק הדואר.

2.4.3. דיווח;

ככל שבכוונת הנהלת בנק הדואר לשנות ו/או לעדכן את נושא ניהול, תפעול והפרדת מערכות המידע המשמשות את בנק הדואר, תדווח ההנהלה על כוונתה למפקח בדיווח מיידי.

3. ניהול סיכוני טכנולוגיות מידע ואבטחת מידע במערכות מידע;

3.1. יעדים;

זיהוי, ניתוח וניהול של כלל הסיכונים הנוגעים לשלמות, זמינות וחסיון נכסי המידע ונכסי טכנולוגיות המידע של הבנק, במטרה למזער את הפגיעה הפוטנציאלית ביעדים ובפעילות העסקית של הבנק, לרבות:

א. סיכונים לשלמות תהליכים עסקיים, הנובעים מהיעדר בקרות נאותות;

ב. סיכונים הנובעים מאיומים טכנולוגיים על נכסי המידע ונכסי טכנולוגיות המידע של הבנק;

ג. סיכונים לשלמות נכסי המידע ונכסי טכנולוגיות המידע, הנובעים מהיעדר בקרות פיזיות וסביבתיות.

3.2. קווים מנחים;

3.2.1. הדירקטוריון יתווה את העקרונות ואת מסגרת העבודה לניהול סיכונים בתחום טכנולוגיות המידע ואבטחת מידע במערכות המידע בכל הנוגע לשירותים הכספיים,

על בסיס מתודולוגיות מקובלות, וכחלק מתוכנית ניהול הסיכונים הכוללת של הבנק;
 3.2.2. לפחות אחת לשנה, יסקור הדירקטוריון את תוכנית ניהול סיכוני טכנולוגיות מידע ואבטחת המידע הנוגעות לבנק. סקירה זו, תתייחס בין היתר, לסיכונים מרכזיים והפעולות הננקטות לשם מזעורם, לאפקטיביות הבקורות הקיימות, ולמעקב אחר התקדמות פעילויות מרכזיות בתחום.

3.3. גיבוש תהליך;

3.3.1. הנהלת הבנק, בהתאם למדיניות הדירקטוריון תפתח ותיישם את מסגרת העבודה לניהול סיכונים בתחום טכנולוגיות המידע, אשר תתייחס, בין היתר, להיבטים הבאים:

3.3.1.1. בהתבסס על מיפוי שירותים עסקיים, וכן נכסי המידע ונכסי טכנולוגיות המידע התומכים בהם (להלן בסעיף 4.1.3.1), יש לזהות סיכונים פוטנציאליים אליהם חשופים כל אחד מתהליכי הליבה, נכסי המידע ונכסי טכנולוגיות המידע;

3.3.1.2. גיבוש מודל המגדיר גורמי סיכון ומדדים להערכת מידת החשיפה הפוטנציאלית, ופרמטרים להערכת מידת אפקטיביות הבקרה;

3.3.1.3. תהליך זה יהיה מתמשך ויעודכן באופן שוטף בהתאם לשינויים במערך הטכנולוגי, בפעילות העסקית ובגורמי הסיכון השונים.

3.3.2. בהתאם לצורך ולכל הפחות אחת לשנתיים, תבחן הנהלת בנק הדואר את הצורך בביצוע התאמות ושינויים במסגרת העבודה לניהול סיכונים בתחום טכנולוגיות המידע הנוגעות לשירותים הכספיים.

3.4. ניהול שוטף;

- 3.4.1** מנהל סיכוני טכנולוגיות מידע יקיים תוכנית ניהול סיכוני טכנולוגיות מידע בנוגע למערכות המידע המשמשות את הבנק, הכוללת בין היתר, את הפעילויות הבאות:
- 3.4.1.1** הערכת מידת הסיכון השורשי לכל אחד מהסיכונים שזוהו (כאמור בסעיף 3.3.1.1);
- 3.4.1.2** הערכת מידת אפקטיביות הבקורות הקיימות ומידת הסיכון השיורי;
- 3.4.1.3** תחזוקה וניטור של תוכנית פעולה למזעור הסיכונים לרמה מקובלת.
- 3.4.2** דגש מיוחד יינתן לניהול סיכונים, הנובעים מיישום ידני של תהליכי ליבה, המבוצעים בין היתר, ללא בקורות אוטומטיות וללא מנגנון רישום פעולות, כנדרש להלן בסעיף 5.2.3.7.
- 3.4.3** בעת שינוי מהותי בסביבה העסקית או במערכות המידע של הבנק, ימפה ויעריך מנהל סיכוני טכנולוגיות המידע סיכונים פוטנציאליים חדשים, תוך תיאום והיוועצות עם מנהל אבטחת מידע ויתר הגורמים הרלבנטיים לשינויים בבנק הדואר. מנהל סיכוני טכנולוגיית המידע ישלב אותם בתוכנית ניהול סיכוני טכנולוגיות המידע.
- 3.4.4** ההנהלה תיזום סקרי סיכונים ו/או מבחני חדירה על פי הצורך, על מנת לבחון את יעילות אמצעי ההגנה והבקרה, אשר יושמו בבנק, הן למערכות התשתית והן למערכות האפליקטיביות של הבנק.
- 3.4.5** הנהלת בנק הדואר תקבע את תדירות הביצוע של סקרי הסיכונים ומבחני החדירה למערכות המידע הנוגעות לשירותים הכספיים. תדירות הביצוע, עבור מערכות מידע המוגדרות כמערכות ליבה או מערכות המכילות מידע רגיש, וכן עבור מערכות מידע החשופות לרשתות ציבוריות, לא תעלה על 18 חודשים. לגבי מערכות אחרות תקבע התדירות, בהתאם לרמת הסיכון אליה חשופה המערכת. תוצאות הסקרים והמבחנים כאמור ידווח למפקח על בנק הדואר במשרד התקשורת ("המפקח").
- 3.4.6** מנהל סיכוני טכנולוגיות המידע יהיה אחראי על תיזמון סקרי הסיכונים ו/או מבחני החדירה, בהתאם להנחיות הנהלת הבנק.
- 3.4.7** מנהל אבטחת המידע בבנק יהיה אחראי על הגדרת תכולת סקרי הסיכונים ומבחני החדירה, בהתאם לסיכונים הידועים, הכלולים בתוכנית ניהול סיכוני טכנולוגיות המידע ובהתייחס לאיומים אחרים.
- 3.4.8** סקרי סיכונים בנושא אבטחת מידע וכן מבחני חדירה ייערכו על ידי גורמים מקצועיים, חיצוניים ובלתי תלויים על מנת למנוע ניגוד עניינים.
- 3.4.9** תוך פרק זמן סביר, תקיים ועדת ההיגוי דיון על ממצאי הסקרים/מבחני החדירה ויקבעו לוחות זמנים לביצוע הפעולות המתקנות.
- 3.4.10** מנהל סיכוני טכנולוגיות המידע ירכז את כלל הממצאים והליקויים, העולים ממקורות שונים, דוגמת: סקרי סיכונים ומבחני חדירה, תרגולים של התוכנית להמשכות עסקית (BCP), דוחות הביקורת הפנימית וכן מהפעילות השוטפת של הגופים השונים בבנק. מנהל סיכוני טכנולוגיות המידע יקיים מעקב אחר תיקון ליקויים אלו, בהתאם ללוחות הזמנים שנקבעו, וידווח על כך, אחת לשנה, להנהלת הבנק ולמפקח.

3.4.11. מנהל סיכוני טכנולוגיות המידע יעדכן את הערכת אפקטיביות הבקורות ואת מידת הסיכון השיורי, כאמור בסעיף 3.4.1.2, בהתאם לממצאים ולאופן הטיפול בהם.

3.5. דיווח;

3.5.1. לפחות אחת לשישה חודשים, ידווח מנהל סיכוני טכנולוגיות המידע להנהלה, על סטאטוס הטיפול בממצאים שעלו בסקרי סיכונים, במבחני חדירה ובדוחות הביקורת הפנימית, וכן על שינויים מהותיים בהערכת הסיכונים.

3.5.2. לפחות אחת לשנה, ידווח מנהל סיכוני טכנולוגיות מידע לדירקטוריון, אודות סיכונים מהותיים שעלו בסקרי סיכונים, במבחני חדירה ובדוחות הביקורת הפנימית, וסטאטוס הטיפול בהם, וכן שינויים מהותיים בהערכת הסיכונים.

3.5.3. יוגדרו אירועים, אשר בגינם נדרש דיווח מידי לגורמים שונים, לרבות: הנהלה, דירקטוריון, הביקורת הפנימית והמפקח.

3.5.4. אחת לשנה ידווח מנהל סיכוני טכנולוגיות מידע למפקח על תוצאות מבחני החדירה, סקרי סיכונים וסטאטוס טיפול בליקויים שהתגלו בדוחות ביקורת פנים, סקרי סיכונים ומבחני חדירה, וכן על שינויים מהותיים בהערכת הסיכונים, בכל הנוגע לשירותים הכספיים.

4. ניהול מידע;

4.1. ניהול נכסי מידע;

4.1.1. יעדים

קיום בקרה נאותה על שלמות, זמינות וחסיין המידע, באמצעות:

- א. ניהול מצאי נכסי המידע של הבנק;
- ב. מינוי גורמים אחראים, עבור כל נכס מידע;
- ג. שילוב בקרות בתהליכי עבודה שונים, הנוגעים לטיפול בנכסי מידע.

4.1.2. קווים מנחים

כחלק ממסמך המדיניות של בנק הדואר (ראה סעיף 2.2.1.2), יאשר הדירקטוריון את מדיניות הבנק בתחום ניהול נכסי המידע. מדיניות זו, תתייחס בין היתר, לכל אחד מהבאים:

4.1.2.1. הגדרת רמות סיווג לנכסי מידע וקביעת הקריטריונים המאפיינים כל

רמה. מידע המוגדר בחוק הגנת הפרטיות כרגיש, או מידע שהוגדר כרגיש על ידי הנהלת הבנק, יוגדר בסיווג גבוה.

4.1.2.2. סיווג של כל מערכת מידע ייקבע לפי סיווג המידע האגור בה.

4.1.2.3. קביעת הקריטריונים להגדרת מערכות מידע כמערכות ליבה.

4.1.2.4. ניהול נכסי המידע, יבוצע בהתאם להוראות הדין לרבות חוק הגנת

הפרטיות ותקנותיו, וסעיפים 188, 188 ו- 88 לחוק הדואר, המתייחסים להגבלה על העברה או הוצאה של מסמכים המשמשים להעברת או הוצאת כספים הנוגעים למתן השירותים הכספיים, שמירת מסמכים ולחובות החלות על בנקאי בדבר שמירת סוד.

4.1.2.5. קביעת אופן ופרק הזמן לשמירת מסמכי מקור בנייר, יבוצע בהתאם

להוראות הדין לרבות תקנות והנחיות ארכיון המדינה לביעור ולשמירה של מסמכים, סעיף 188 לחוק הדואר המתייחס לחובות החלות על בנק הדואר בנושא שמירת מסמכים, וכן דרישות צו איסור הלבנת הון.

4.1.2.6. על מנת להבטיח את מהימנות ושלמות המידע בעת העברת מידע

בממשקים מ/אל ספקים ושותפים עסקיים, ובהתאם להערכת סיכונים, יש ליישם עקרונות אבטחה מקובלים לרבות בקרת גישה, הצפנה, והגדרת פעולות בקרה נדרשות.

4.1.3. גיבוש התהליך;

4.1.3.1. מנהל מערכות המידע יהיה אחראי על תיעוד כלל שירותי הבנק ומיפוי

נכסי המידע ונכסי טכנולוגיות המידע, המשמשים בכל אחד מהשירותים. תיעוד זה יכלול, בין היתר, את זהות בעל המידע, התייחסות לרמת הסיווג של המידע המאוחסן בכל מערכת, האם

מדובר בשירותים אותם מספק הבנק בתקשורת, האם מדובר במערכת ליבה, וכן את מידת הזמינות הנדרשת בחירום.

4.1.3.2 מנהל מערכות המידע יהיה אחראי על מיפוי הממשקים והתשתית הטכנולוגית, המשמשים לקישור מערכות המידע של בנק הדואר למערכות מידע של לקוחות ושותפים עסקיים.

4.1.3.3 בעל מידע - עבור כל נכס מידע, תמנה הנהלת הבנק גורם מהתחום העסקי, ותגדיר את תחומי סמכותו ואחריותו, לרבות: סיווג הנכס, הגדרת הזמינות הנדרשת בחרום, יידוע נאמן המידע באשר להנחיות מיוחדות לטיפול בנכס המידע ומתן אישור ותיקוף של הרשאות גישה לנכס המידע, כמפורט להלן בסעיף 5.3.

4.1.3.4 נאמן המידע - מנהל מערכות מידע של הבנק, יוגדר כנאמן המידע. בין היתר, ובמידת הצורך, אחראי נאמן המידע, להסב את תשומת ליבו של בעל המידע, באשר לליקויים וחריגות מנהלי הבנק או מתהליכי עבודה מקובלים.

4.1.4 ניהול שוטף;

4.1.4.1 נכסי המידע השונים יתויגו באופן ברור, בהתאם לרמות הסיווג שהוגדרו (ראה סעיף 4.1.2.1 לעיל).

4.1.4.2 באחריות מנהל מערכות מידע, לתחזק באופן שוטף את רשימת נכסי המידע ולעדכן אותה, בהתאם לשינויים ולהנחיות בעלי המידע.

4.1.4.3 באחריות מנהל מערכות המידע, להבטיח כי הנתונים השמורים במערכות המידע מהימנים ושלמים, ובמידת הצורך לפעול למען טיובם.

4.1.4.4 אחת ל-18 חודש לפחות, יש לבחון כי אמצעי האבטחה והבקורות על המידע המועבר בממשקים השונים, תואמים את רגישות המידע והסיכונים הפוטנציאליים.

4.1.5 דיווח;

4.1.5.1 לפחות אחת לשנה, יעביר מנהל מערכות מידע את רשימת נכסי המידע, הכוללת בין היתר את פירוט המידע המופיע בסעיף 4.1.3.1 לעיל, לסקירה ואישור של וועדת ההיגוי.

4.1.5.2 לפחות אחת לשנה, יעביר מנהל מערכות מידע את רשימת הממשקים, כאמור בסעיף 4.1.3.2 לעיל, לסקירה ואישור של וועדת ההיגוי.

4.2. ניהול שינויים;

4.2.1. יעדים:

גיבוש תהליך סדור ומבוקר לביצוע שינויים בנכסי מידע ונכסי טכנולוגיות המידע, העונים על דרישות עסקיות, במטרה להבטיח את מהימנות, זמינות ושלמות הנתונים בסביבת הייצור.

4.2.2. קווים מנחים:

על הנהלת הבנק, לגבש תהליך לביצוע שינויים בכלל נכסי המידע ונכסי טכנולוגיות מידע הנוגעים לשירותים הכספיים, אשר יכלול, בין היתר, התייחסות להיבטים הבאים:

4.2.2.1. הגדרת שלבים ובקורות הכלולים בתהליך השינוי, בהתאם לפרקטיקה

מקובלת;

4.2.2.2. סמכותם ואחריותם של הגורמים המעורבים בייזום, אישור, ביצוע

בפועל ובקרת תהליך השינוי, כך שיעמוד בקריטריונים של הפרדת

תפקידים;

4.2.2.3. קביעת קריטריונים למקרים בהם יש לבצע שינוי חרום, והגדרת

השלבים והבקורות, בעת ביצוע שינוי חרום;

4.2.2.4. קביעת מעורבותו של מנהל אבטחת מידע של בנק הדואר בתהליך,

לרבות הגדרת קריטריונים למקרים בהם יהווה גורם מאשר ולמקרים

בהם יהווה גורם מידע בלבד;

4.2.2.5. הפרדת סביבת הייצור מסביבות הפיתוח והבדיקות.

4.2.3. גיבוש תהליך;

4.2.3.1. בהתאם לקווים מנחים, יישם מנהל מערכות מידע תהליך ניהול שינויים

סדור, הכולל בקורות ותיעוד הולם, עבור כל אחד משלביו;

4.2.3.2. כחלק מיישום תהליך ניהול שינויים, יש לכלול התייחסות לביצוע שינויי

חירום;

4.2.3.3. מנהל מערכות מידע יוודא כי תהליך שינוי, בו מעורבים גם ספקים

חיצוניים, יתבצע בהתאם לתהליך הקיים בבנק;

4.2.3.4. עבור כל מערכת ליבה, יוקמו סביבות פיתוח ובדיקות, בנפרד מסביבת

הייצור. הרשאות גישה לסביבות אלו יינתנו בהתאם לעקרונות

מקובלים להפרדת תפקידים.

4.2.4. ניהול שוטף;

4.2.4.1. מנהל מערכות מידע יגבש תהליך פיקוח ומעקב על סטאטוס בקשות

השינויים;

4.2.4.2. מנהל אבטחת מידע של הבנק, יבטיח כי המידע המועבר מסביבת

הייצור לסביבת הפיתוח והבדיקות לא ייחשף לגורמים שאינם מורשים;

4.2.4.3. כל שינוי מהותי בתחום טכנולוגיות המידע יקבל התייחסות בתוכנית

ניהול סיכוני טכנולוגיות מידע ובתוכנית ההמשכיות העסקית.

4.2.5. דיווח;

- 4.2.5.1** לאחר סיום ביצוע השינוי ואישורו וטרם העברתו לסביבת הייצור, יש לעדכן את המשתמשים אודות מהות השינוי והשפעתו.
- 4.2.5.2** אחת לשנה ידווח מנהל מערכות המידע של הבנק לוועדת ההיגוי, באשר להיקף השינויים אשר בוצעו בשנה החולפת, לרבות ציון מספר השינויים, ומספר התקלות כתוצאה משינויים אלו.
- 4.2.5.3** אחת לשנה ידווח מנהל מערכות המידע של הבנק לוועדת ההיגוי, באשר להיקף השינויים אשר בוצעו בשנה החולפת, לרבות ציון מספר השינויים, ומספר התקלות כתוצאה משינויים אלו.

4.3. גיבוי ושחזור נתונים;

4.3.1. יעדים:

קיום תהליך גיבוי מבוקר, של כלל נכסי המידע, אשר יבטיח את זמינותם, בעקבות אירועי כשל נקודתיים.

4.3.2. קווים מנחים:

בהתאם לצרכים עסקיים, על הנהלת הבנק, להגדיר עקרונות בנושא גיבוי ושחזור נתונים, אשר יכלול בין היתר התייחסות להיבטים הבאים:

4.3.2.1. גיבוי כלל נכסי המידע וכן הגדרות מערכת של נכסי טכנולוגיות המידע

השונים;

4.3.2.2. מחזוריות תהליך הגיבוי לרבות סוג הגיבוי ומשך הזמן לשמירת מצעי

גיבוי לפני מחזורם;

4.3.2.3. אחסון מצעי גיבוי, מחוץ לאתרי הארגון (off-site) במרחק אשר יקטין

את ההסתברות לכך ששני האתרים יפגעו מאותו אירוע, ולכל הפחות, מחוץ למרחב העירוני של אתר הייצור;

4.3.2.4. אופן האחסון של מצעי גיבוי, הן בארגון והן מחוצה לו, כך שיקיים

קריטריונים הנוגעים לאבטחה פיזית וסביבתית;

4.3.2.5. עקרונות ליישום בקרות על תהליך הגיבוי, לרבות בדיקת תקינות

הגיבוי לאחר סיומו;

4.3.2.6. הגדרת היקף ותדירות, לביצוע ניסיונות שחזור יזומים.

4.3.3. יישום:

4.3.3.1. בהתאם לעקרונות המנחים, יגבש מנהל מערכות מידע תהליך, אשר

יבטיח כי כלל נכסי המידע בבנק מגובים כנדרש וכי נכסי מידע חדשים, ישולבו בתהליך כנדרש.

4.3.4. ניהול שוטף:

4.3.4.1. על מנהל מערכות מידע לבצע פיקוח ומעקב שוטפים על תקינות

תהליך הגיבוי;

4.3.4.2. בהתאם לעקרונות אשר הוגדרו בתחום, על מנהל מערכות מידע לבצע

בדיקות שחזור יזומות באופן תקופתי;

4.3.4.3. לפחות אחת לשנה, על מנהל מערכות מידע לתקף את רשימת נכסי

המידע הכלולים בתהליך הגיבוי, על מנת להבטיח כי כלל נכסי המידע של הבנק מגובים כנדרש.

דיווח:

4.3.4.4. אחת לשנה, ידווח מנהל מערכות מידע לוועדת ההיגוי, אודות שינויים או ליקויים מהותיים בתהליך הגיבוי והשחזור וכן אודות תהליך התיקוף השנתי של רשימת נכסי מידע, הנכללים בתהליך הגיבוי.

5. תפעול מערך אבטחת מידע;

5.1. אבטחה פיזית וסביבתית:

5.1.1. יעדים

הגנה על נכסי מידע ונכסי טכנולוגיות המידע, לרבות מסמכי מקור בפורמט נייר, על מנת להפחית את הסיכון להפרעות בפעילות העסקית השוטפת ומניעת גישה פיזית לא מורשת אליהם.

5.1.2. קווים מנחים:

על הנהלת הבנק להתוות עקרונות בתחום האבטחה הפיזית והסביבתית אשר יכללו, בין היתר, התייחסות להיבטים הבאים:

5.1.2.1. קביעת קריטריונים לרמת רגישות של אזורי עבודה על סמך רגישות

המידע הנשמר בכל אזור;

5.1.2.2. בהתאם להערכת הסיכונים, יוגדרו בקרות גישה פיזיות לכל רמת

רגישות של אזורי עבודה;

5.1.2.3. אפיון בקרות סביבתיות בחדר המחשב, בהתאם לפרקטיקה המקובלת

ולהערכת הסיכונים;

5.1.2.4. הגדרת תהליך מאובטח לטיפול בנכסי מידע פיזיים לרבות מסמכי נייר

ומדיה מגנטית המכילים מידע רגיש, כאמור בסעיף 4.1.2.1 לעיל.

לרבות התייחסות להיבטים הבאים: סריקה, גניזה, גריסה והשמדה.

5.1.3. גיבוש תהליך:

5.1.3.1. מיפוי אזורי עבודה הכוללים נכסי מידע רגישים;

5.1.3.2. יישום בקרות גישה, בהתאם לרמת רגישות של כל אזור;

5.1.3.3. הגדרת מורשי גישה לכל אזור בהתאם לצרכים עסקיים;

5.1.3.4. יישום בקרות סביבתיות בחדר המחשב, על מנת להגן על נכסי המידע

ונכסי טכנולוגיות המידע, ולשמור על זמינותם;

5.1.3.5. הנהלת הבנק תיישם תהליך לטיפול בצידוד ומסמכי נייר בהתאם לקווים

המנחים, כאמור בסעיף 4.1.2.5 לעיל.

5.1.4. ניהול שוטף:

5.1.4.1. אחת לשנתיים, או לפני שינוי מהותי, יבחן מנהל אבטחת מידע בבנק

ובשיתוף אגף הביטחון של החברה את מידת ההתאמה של הבקרות

הפיזיות והסביבתיות בחדר המחשב לצרכי הבנק;

5.1.4.2. אחת לשנה יתקף מנהל אבטחת מידע של הבנק את רשימת מורשה

הכניסה לאזורים ממודרים.

5.1.4.3. אגף הביטחון יהיה אחראי על ביצוען בפועל של בדיקות תקינות

תקופתיות לבקרות הפיזיות והסביבתיות בחדרי מחשב, בהתאם

לתדירות הנדרשת.

5.1.4.4. ממונה אבטחת מידע בבנק יודא את קיומן של בדיקות אלו כנדרש.

5.1.5. דיווח:

5.1.5.1. על ממצאי בדיקת התיקוף ידווח מנהל אבטחת מידע של הבנק לאגף הביטחון בחברה.

5.2. ניהול תקשורת ותפעול;

5.2.1. יעדים:

א. הגנה על רשתות התקשורת של הבנק, נכסי המידע ונכסי טכנולוגיות המידע המקושרים אליהן, באמצעות מידור רשתות ויישום בקרות נאותות, בהתאם לסיכונים להם חשופה כל רשת;

ב. מניעת זליגת מידע בערוצי תקשורת שונים, לרבות דואר אלקטרוני ומצעי זיכרון נתיקים;

ג. הבטחת תגובה מהירה ויעילה בעקבות התרחשות אירוע אבטחת מידע, המשבש את פעילות הבנק.

5.2.2. קווים מנחים:

על הדירקטוריון לגבש ולאשר את מדיניות בנק הדואר בתחומים הבאים:

5.2.2.1. הגדרת פעולות מותרות לעובדי הבנק ברשת האינטרנט, על פי הערכת סיכונים ותוך נקיטת אמצעי בקרה נאותים;

5.2.2.2. גיבוש מדיניות גישה מרחוק, מרשתות ציבוריות ואחרות, אל נכסי המידע ונכסי טכנולוגיות המידע של הבנק;

5.2.2.3. גיבוש מדיניות בנוגע להצפנת מידע השמור במערכות המידע או המועבר אל גורמי חוץ;

5.2.2.4. הגדרת השימושים המותרים, והבקרה על מצעי זיכרון נתיקים;

5.2.2.5. היערכות למתן תגובה נאותה, לאירועי אבטחת מידע.

5.2.3. גיבוש תהליך:

מנהל מערכות מידע יהיה אחראי על יישומן של בקרות אבטחת מידע, המפורטות להלן.

5.2.3.1. חלקי הרשת השונים ימודרו באמצעים לוגיים או פיזיים, בהתאם למידת החשיבות והרגישות של המערכות.

5.2.3.2. קישוריות עובדי הבנק לרשת האינטרנט מתחנות עבודה תתאפשר בהתקיים אחד מאלה:

א. תחנת העבודה קשורה אך ורק לרשת אינטרנט או לרשת שקשורה אך ורק לרשת אינטרנט ואין עליה יישומים בנקאיים או מידע שאינו פומבי;

ב. הקישוריות לרשת אינטרנט תיעשה באמצעות שרת ייעודי, אשר ימוקם ברשת החיצונית של הבנק, ומאפשר ביצוע פעולות ברשת האינטרנט באופן מאובטח;

5.2.3.3 קישוריות של רשת בנק הדואר לרשת אינטרנט, תאובטח באמצעים מתאימים ולכל הפחות על ידי אנטי-וירוס, מסנני תוכן (Content-Filtering), מערכת למניעת ניסיונות חדירה (IPS) ו-Firewall;

5.2.3.4 גישה מרחוק, תתבצע אל מול רכיב אבטחת מידע ייעודי, התומך בהזדהות חזקה ומספק את התשתית להצפנת תווך התקשורת. בנוסף, יופעל על רכיב זה מנגנון האוכף מדיניות, באשר לדרישות הסף מהתחנה המרוחקת המנסה להתחבר לרשת הבנק. התחברות מרחוק לא תתאפשר לתחנות אשר אינן עומדות בדרישות סף אלו.

5.2.3.5 הקישור של רשת הבנק, לגורמים חיצוניים שונים, דוגמת סניפי חברת הדואר, שותפים עסקיים, ספקים ולקוחות, יהיה מבוקר באמצעות רכיבים מתאימים, המאפשרים בקרת גישה וסינון תוכן. במקרה של קישורים בעלי רגישות גבוהה, יש לבחון את הצורך במערכת למניעת ניסיונות חדירה (IPS).

5.2.3.6 בחינת הצורך בהצפנת נתונים, במערכות שהוגדרו כמערכות ליבה או במערכות המכילות מידע בסיווג גבוה, ובלבד שבמקרים הבאים תתקיים הצפנה:

א. שירותי בנקאות בתקשורת באמצעות רשת האינטרנט;

ב. גישה מרשתות ציבוריות למחשבי בנק הדואר;

ג. סיסמאות של מורשי גישה;

ד. העברת מידע רגיש מחוץ לבנק;

ה. אמצעי מחשוב ניידים, לרבות טלפונים ניידים.

5.2.3.7 על מנת לאתר פעילויות לא מורשות, יש ליישם מנגנון נתיב בקרה (audit trail) בכלל המערכות, אשר יכלול בין היתר תיעוד אודות מהות הפעולה, זהות המבצע, מקור הגישה וזמן הגישה. כמו כן, נתיב הבקרה יכלול מידע אשר יאפשר לגלות ניסיונות גישה לא מורשים שנחסמו.

5.2.3.8 פיתוח מנגנון תגובה לתקריות אבטחת מידע, אשר יכלול הגדרת סוגי פעילויות ואירועים שלגביהם יש לספק התראה לגורמים המוסמכים. תוגדר חלוקת אחריות להערכה, לתגובה ולניהול של תקריות אבטחה. כמו כן, יכלול המנגנון נהלי דיווח על אירועי אבטחת מידע.

5.2.3.9 מנהל אבטחת מידע של הבנק יודא קיום כל האמור לעיל.

5.2.4. ניהול שוטף:

5.2.4.1. אחת לתקופה יבחן מנהל אבטחת המידע בבנק הדואר את מידת ההתאמה של בקורות אבטחת המידע הקיימות בכול הנוגע לשירותים הכספיים ולמערכות המידע של הבנק וימליץ, לאחר התייעצות עם מנהל אבטחת מידע בבנק ומנהל סיכוני טכנולוגיית מידע, על עדכון, בהתאם לשינויים במפת הסיכונים.

5.2.4.2. על מנת לוודא, כי אירועים חריגים הנרשמים ברכיבי אבטחת המידע השונים ובנתיבי הבקרה של מערכות המידע יקבלו טיפול הולם ומהיר, יש ליישם מערכת מתאימה, אשר תרכז אירועים מהמערכות השונות, ותתריע על אירועים חריגים.

5.2.5. דיווח:

5.2.5.1. אחת לשנה, ידווח מנהל אבטחת המידע של בנק הדואר לוועדת ההיגוי, אודות פרויקטים מרכזיים, אירועים חריגים ושינויים מהותיים במפת הסיכונים, הנוגעים למערך התקשורת והתפעול בכל הנוגע לשירותים הכספיים.

5.2.5.2. אחת לשנה, ידווח מנהל סיכוני טכנולוגיית מידע לוועדת ההיגוי, אודות פרויקטים מרכזיים, אירועים חריגים ושינויים מהותיים במפת הסיכונים הנוגעים למערך התקשורת והתפעול בכל הנוגע לשירותים הכספיים.

5.3. בקרת גישה;

5.3.1. יעדים:

מידור הגישה לנכסי מידע, לשם מניעת חשיפת מידע לגורמים לא מורשים, ושימוש באמצעי אימות נאותים, התואמים את הסיכונים הפוטנציאליים ואת רמת הסיווג של נכס המידע.

5.3.2. קווים מנחים:

הנהלת הבנק, תגבש עקרונות ליישום בקורות גישה לנכסי המידע ולנכסי טכנולוגיות המידע, אשר כוללות בין היתר, התייחסות להיבטים הבאים:

5.3.2.1. הצורך באמצעי זיהוי חד-ערכי ואישי, לכל מורשה גישה לנכסי המידע ולנכסי טכנולוגיות המידע, הן לעובדי הבנק והן לגורמים אחרים;

5.3.2.2. שימוש בסיסמאות מורכבות, לאימות גישה המתבצעת לנכסי המידע ולנכסי טכנולוגיות המידע של הבנק, לרבות: אורך מינימאלי, שילוב של סוגי תווים שונים, תוקף הסיסמא ונעילת חשבון;

5.3.2.3. שימוש באמצעי אימות חזק, לאימות גישה המתבצעת מרשת חיצונית, אל רשת הבנק;

5.3.2.4. הקצאת הרשאות גישה, על בסיס עקרון "הצורך-לדעת", ובאישור הגורמים המוסמכים.

5.3.3 גיבוש תהליך:

- על מנת להשיג יעדים אלו, על מנהל מערכות מידע לבצע בין היתר את הפעולות הבאות:
- 5.3.3.1 גיבוש תהליך מבוקר ומתועד, המטפל בהקצאת הרשאות וביטולן בהתאם לתפקיד ולצורך, לאורך מחזור חיי חשבון משתמש: הקמה, שינוי וסגירה;
 - 5.3.3.2 הגדרת הגורמים הנדרשים לאשר בקשה להקצאת הרשאות גישה, לרבות בעל המידע, כפי שהוא מוגדר בסעיף 4.1.3.3 לעיל;
 - 5.3.3.3 יישום בקרה טכנולוגית לאכיפת מדיניות הסיסמאות, במערכות השונות;
 - 5.3.3.4 גיבוש תהליך מבוקר ומאובטח לטיפול בסיסמאות, לרבות מסירה ראשונית למשתמש ושינוי סיסמא לבקשת משתמש;
 - 5.3.3.5 יישום מנגנון ניתוק התקשורת למערכת ליבה או מערכת המכילה מידע בסיווג גבוה, לאחר פרק זמן של אי פעילות במערכת;
 - 5.3.3.6 גיבוש נוהל שימוש במידע, המתאר בין היתר, את חובותיו של עובד באשר לחיסיון המידע אליו הוא חשוף, ואופן שמירת פרטים אודות חשבונות וסיסמאות גישה.

5.3.4 ניהול שוטף:

- 5.3.4.1 עובדי בנק הדואר, להם תינתן גישה לנכסי המידע של הבנק, יוחתמו על נוהל שימוש במידע;
- 5.3.4.2 הקצאה או גריעה של הרשאות, יתבצעו בהתאם לתהליך המתואר בסעיף 5.3.3.1 לעיל;
- 5.3.4.3 אחת לחצי שנה יקיים מנהל מערכות המידע תהליך תיקוף הרשאות גישה, במסגרתו יאשר כל בעל מידע את רשימת מורשי הגישה לנכס המידע המצוי באחריותו.

5.3.5 דיווח:

- 5.3.5.1 אחת לחצי שנה ידווח מנהל מערכות המידע לוועדת ההיגוי על ביצוע תהליך תיקוף ההרשאות, תוך התייחסות לממצאי תהליך התיקוף.

6. רציפות במתן שירותים;

6.1. יעדים:

מטרת התוכנית להמשכיות עסקית (BCP), הינה השבתם לכשירות מלאה של שירותים עסקיים, אותם נדרש הבנק לספק, בעקבות התקיימות תרחישי קיצון כגון: כשלים טכנולוגיים, טעויות אנוש, אסונות טבע ומצבי חירום לאומיים, בדגש על שירותים כספיים בסיסיים.

6.2. קווים מנחים:

6.2.1 על הדירקטוריון להתוות עקרונות ליישום תוכנית המשכיות עסקית (BCP), אשר

תבטיח רציפות במתן שירותים בבנק הדואר. על התוכנית להתייחס בין היתר להיבטים הבאים:

6.2.1.1 קיום תהליך ניתוח השלכות עסקיות (BIA), להערכת הסיכונים

והשפעה הפוטנציאלית של תרחישים שונים על שירותי הבנק;

6.2.1.2 תהליך ניתוח השלכות עסקיות (BIA) יתבסס על מיפוי התהליכים,

מיפוי נכסי המידע ונכסי טכנולוגיות המידע התומכים בהם, כנדרש לעיל בסעיף 4.1.3.1;

6.2.1.3 תוצאות תהליך ניתוח השלכות עסקיות (BIA), יהוו בסיס

לקביעת RTO, RPO, RLO, MTPOD עבור כל שירות של הבנק ובפרט עבור שירותים כספיים בסיסיים, ועבור כל נכס מידע ונכס טכנולוגיות מידע, התומך בשירותים אלו;

6.2.1.4 קביעת מאפייני אתר החרום, לרבות מיקומו באופן שתוקטן

ההסתברות לכך ששני האתרים יפגעו מאותו תרחיש, ולכל הפחות, מחוץ למרחב העירוני של אתר הייצור;

6.2.1.5 קיום תרגילים והדרכות עובדים, לבחינת תקינותה ומידת התאמתה של

התוכנית, לצרכי הבנק.

6.2.2 על מנת לעמוד ביעד המרכזי של תוכנית המשכיות עסקית (BCP) - השבתם

לכשירות מלאה של כל שירותי הבנק - תקיף התוכנית, בין היתר, את שני השלבים הבאים:

6.2.2.1 השבתם לפעילות חלקית של כל שירותי הבנק, תוך עמידה בדרישות

RTO, RPO ו-RLO אשר הוגדרו עבורם;

6.2.2.2 השבתם לפעילות מלאה (RLO=100%) של כל שירותי הבנק, תוך

עמידה בדרישות MTPOD אשר הוגדרו עבורם.

6.2.3 הדירקטוריון יפקח על תהליך הגיבוש והתחזוקה השוטפת של תוכנית ההמשכיות

העסקית (BCP) ויאשר אותה, כך שתבטיח רציפות במתן שירותים בבנק הדואר.

6.3. גיבוש תהליך:

6.3.1. על הנהלת בנק הדואר לגבש תכנית המשכיות עסקית (BCP) למתן שירותים רציפים בבנק הדואר אשר תכלול בין היתר, התייחסות למרכיבים הבאים:

6.3.1.1. הגדרת תנאים וגורמים מוסמכים להפעלת תוכנית ההמשכיות העסקית (BCP);

6.3.1.2. מינוי מנהל המשכיות עסקית והגדרת תחומי סמכות ואחריות, בשגרה ובעת חרום, לרבות שמירה על עדכנות תוכנית ההמשכיות העסקית (BCP), תירגולה וכן דיווח תקופתי לדירקטוריון ולהנהלת הבנק.

6.3.1.3. הגדרת סמכות ואחריות של בעלי תפקידים בשגרה ובחירום לרבות בעלי תפקידים האמונים על יישום הפתרון הטכנולוגי, והגדרת בעלי תפקידים חילופיים לפונקציות חיוניות בבנק הדואר;

6.3.1.4. עבור כל שירות של הבנק, יוגדרו הפרמטרים הבאים: RLO, MTPOD, RTO, RPO, בהתאם לתוצרי תהליך ניתוח השלכות עסקיות (BIA).

6.3.1.5. יחד עם זאת, יבטיח הבנק חזרה לפעילות, תוך פרק זמן של עד 12 שעות (RTO), של כל אחד מהשירותים הבאים:

א. שירותים כספיים בסיסיים, המתוארים בחלק ב' לתקנות שירותים כספיים בסיסיים בסעיפים 22, 23, 24, 25, 27, 28, 29, 30, 33.

ב. וכן, שירותים כספיים בסיסיים המהווים חלק מסעיף 21 בתקנות שירותים כספיים בסיסיים: "...קבלת מידע בנוגע לחשבון סילוקים באשנב, באמצעות משלוח בדואר, באמצעות מענה קולי או דרך אתר אינטרנט; הנפקת פנקס שיקים; הנפקת כרטיסי חיוב, חידוש וטיפול באבדנו".

6.3.1.6. בהתאם לפרמטרים אשר הוגדרו בסעיפים 6.3.1.4 ו- 6.3.1.5 לעיל, יגובשו תהליכים ונהלים להפעלת כל שירותי הבנק והמערך הטכנולוגי בחירום.

6.3.1.7. גיבוש נהלי תקשורת מול גורמים רלוונטיים לבנק בשעת חירום, לרבות עובדים, ספקים, לקוחות, רשויות פיקוח ועוד.

6.3.1.8. שימוש בתהליכי עבודה ידניים, כחלק מתוכנית המשכיות עסקית (BCP), יאושרו מראש על ידי הדירקטוריון. במקרים אלה, יוודא הבנק את חיזוקם של מעגלי הבקרה.

6.3.2. בהתאם לניתוח הצרכים, תיישם הנהלת בנק הדואר תוכנית התאוששות טכנולוגית (DRP), אשר תאפשר להשיב לפעולה את נכסי טכנולוגיות המידע התומכים בכל שירותי הבנק השונים.

6.3.2.1. בהסתמך על רשימת נכסי המידע ונכסי טכנולוגיות המידע הקיימת בבנק הדואר (ראה סעיף 4.1.3.1 לעיל), ובהתייחס לפרמטרים אשר

- הוגדרו בסעיפים 6.3.1.4 ו- 6.3.1.5 לעיל, יגובשו עקרונות התוכנית ואופי הפתרון הטכנולוגי.
- 6.3.2.2.** תוכנית ההתאוששות הטכנולוגית (DRP), תספק מענה, הן לשלב ההתאוששות הראשוני והן לשלב ההתאוששות המלאה, והיא תתייחס, בין היתר, למיקומו של אתר החרום, לרמת המוכנות שלו ולהיקף השירותים הזמינים לבנק, במהלך השהות בו.
- 6.3.3.** ההנהלה תוודא כי הסכמי התקשרות עם ספקים חיצוניים רלוונטיים, יכללו בין היתר התייחסות הולמת למצב של הפרעה לפעולה סדירה של מערכות המידע, בין אם בחצרי הבנק ובין אם אצל ספק השירות. כמו כן, יש לוודא כי הסכמי ההתקשרות עם ספקי השירות מהותיים, יבטיחו עמידה של הספק, בהגדרות RTO ו- RPO אותן קבע בנק הדואר (ראה להלן סעיף 7.3.3.6)
- 6.3.4.** על ההנהלה לגבש תהליך לזיהוי לקוחות חסרי תיעוד רשמי, אשר יתייחס בין היתר לנושאים הבאים:
- 6.3.4.1.** גיבוש נהלים לצורך זיהוי ואימות לקוחות חסרי תיעוד רשמי, ובתוך כך אבחנה בין בעלי חשבון סילוקים בבנק לבין לקוחות חסרי חשבון. הנהלים יכללו, בין היתר, התייחסות ספציפית לתשלום קצבאות ביטוח לאומי וממשלה ללקוחות מזדמנים.
- 6.3.4.2.** גיבוש מדרג לאמצעי זיהוי חילופיים דוגמת מסמכים רשמיים של המדינה או תיעוד חלופי כגון: תעודת סטודנט, כרטיס אשראי, כרטיס קופת חולים וכיוצא באלה. בהיעדר תעודה מזהה המכילה פרטים אלו, יש לבחון את השימוש באפשרויות הבאות, לצורך זיהוי הלקוח:
- א. מסמכי זיהוי שנסרקו ונשמרו מראש על ידי הבנק;
- ב. דוגמת חתימה של הלקוח;
- ג. אימות זהות הלקוח באמצעות תשאל הלקוח - אודות מידע הקיים בבנק. על הבנק לטייב באורח שוטף ורציף את המידע כאמור.
- 6.3.4.3.** בהתאם להערכת סיכונים, יוגדרו סוגי השירותים וסכומי העסקאות אותם ניתן לבצע.
- 6.3.5.** הנהלת בנק הדואר תקבע את אופן ותדירות ההדרכות, אשר יועברו לגורמים השונים האמונים על יישום התוכנית;
- 6.3.6.** הנהלת בנק הדואר תקבע את תדירות ביצוע תרגילי התאוששות, היקפם ותוכנם. לכל הפחות יבוצע תרגיל אחת לשנה.
- 6.4. ניהול שוטף:**
- 6.4.1.** על הנהלת בנק הדואר לוודא את קיומו של תהליך ריענון עבור העובדים הרלוונטיים, בדבר פרטי התוכנית להמשכיות עסקית (BCP). ריענון כאמור יתייחס, בין היתר, לנהלי עבודה בחירום, וכן לתפקידים ותחומי אחריותם בחירום.

- 6.4.2.** כאמור בסעיף 6.3.6 לעיל, תבצע הנהלת בנק הדואר תרגול של התוכנית להמשכיות עסקית (BCP). עבור כל תרגיל, יוגדרו מראש יעדים ומטרות ותוצאותיו יתועדו. עבור כל ליקוי שיתגלה, יוגדר לוח זמנים לטיפול.
- 6.4.3.** מנהל סיכוני טכנולוגיות המידע יקיים מעקב אחר הטיפול בליקויים אלו, בהתאם לאמור בסעיף 3.4.10 לעיל.
- 6.4.4.** על הנהלת בנק הדואר לבחון את נאותות תוכנית ההמשכיות העסקית (BCP) לפעילות הבנק, לפחות אחת ל - 18 חודשים, או לפני ביצוע שינוי מהותי בתהליך עסקי או במערך טכנולוגי המידע.

6.5. דיווח:

- 6.5.1.** אחת לשנה ידווח מנהל ההמשכיות העסקית, להנהלת הבנק ולדירקטוריון, בנושא תוכנית ההמשכיות העסקית (BCP). דיווח זה יתייחס, בין היתר, לתוכן והיקף התרגילים שבוצעו, לתוצאות התרגילים, וכן לסטאטוס הפעולות המתקנות.
- 6.5.2.** בעת הפעלת תוכנית המשכיות עסקית (BCP), או חלקים ממנה, יש לדווח למפקח באופן מיידי.

7. מיקור חוץ;

7.1. יעדים:

מיקור-חוץ בתחום טכנולוגיות מידע, חושף את בנק הדואר לסיכונים פוטנציאליים נוספים, מעבר לסיכונים הגלומים בפעילות עסקית המנוהלת באמצעות גורמים פנימיים. הנהלת הבנק תזהה סיכונים אלה ותנהל אותם באופן אפקטיבי כך שיעמדו הן בדרישות עסקיות והן בדרישות אבטחת מידע. לצורך כך יקיים בנק הדואר בין היתר, בקרה נאותה על:

- א. הסכמים עם גורמי חוץ;
- ב. מעקב שוטף אחר עמידת הספק בדרישות שהוגדרו בהסכם;
- ג. ניטור שוטף של השירותים המסופקים על ידי גורמים חיצוניים.

יודגש כי הוצאת שירותים למיקור חוץ, אינה גורעת מאחריות הנהלת בנק הדואר לכל פעולה שנעשית מטעמה על ידי גורמים חיצוניים.

7.2. קווים מנחים:

כחלק ממדיניות טכנולוגיות מידע, על הדירקטוריון לקבוע עקרונות להתקשרות עם ספקי מיקור חוץ, אשר יכללו בין היתר, התייחסות להיבטים הבאים:

- 7.2.1. בהתבסס על הערכת הסיכונים, יש לקבוע אילו סוגי פעילויות ניתן לבצע באמצעות גורמים חיצוניים;
- 7.2.2. קביעת קריטריונים עסקיים בהם נדרש לעמוד ספק שירותי מערכות מידע, לרבות מיומנות, מקצועיות, וחוסן כלכלי;
- 7.2.3. גיבוש מנגנוני שליטה ובקרה על פעילות המבוצעת באמצעות מיקור חוץ.

7.3. גיבוש תהליך:

7.3.1. הנהלת בנק הדואר תוודא את מימושם של העקרונות הבאים, כחלק מהליך התקשרות עם ספק שירותי חיצוני או שותף עסקי של הבנק:

- 7.3.1.1. ווידוא עמידה בעקרונות להתקשרות עם ספקי מיקור חוץ, כפי שקבע הדירקטוריון;
- 7.3.1.2. עמידה בעקרונות אבטחת מידע המקובלים בבנק.
- 7.3.2. הנהלת בנק הדואר תאשר התקשרויות מהותיות עם ספקי מיקור חוץ בתחום טכנולוגיות המידע ואבטחת מידע במערכות המידע, הנוגעים לשירותים הכספיים.
- 7.3.3. יש לעגן את העקרונות המופיעים בפרק זה, במסגרת הסכם התקשרות כתוב, אשר יתייחס בין היתר לבאים:
 - 7.3.3.1. הגדרת תחומי אחריות של כל אחד מהצדדים להסכם, לרבות קבלני משנה של כול אחד מהצדדים;
 - 7.3.3.2. הגדרת הסכם רמת שירות SLA, ולפי העניין הסכם רמת תפעול OLA;
 - 7.3.3.3. חובת סודיות;

- 7.3.3.4.** הסכמת הספק לביצוע ביקורות בחצרו מטעם הבנק. לחילופין, רשאי הבנק להתבסס על הסמכה של הספק לתקנים מקובלים בתחום דוגמת SAS70, SSAE16 או תקן דומה, זאת לאחר שבחן את פרטי ההסמכה ומצא כי היא עונה על דרישותיו;
- 7.3.3.5.** הסדרים לאירועים ומצבים מהותיים, לרבות למצב בו ידרשו הצדדים לסיום מוקדם של חוזה התקשרות ביניהם;
- 7.3.3.6.** אופן מתן שירותי מיקור חוץ מהותיים והיקפם, בעקבות אירוע אסון כמתואר בסעיף 6.3.3 לעיל.
- 7.3.4.** יש לגבש מנגנוני דיווח של ספקי שירותים מהותיים, במתכונת ותדירות, התואמת את היקף פעילותו של הספק ואת מידת החשיבות של השירות לבנק.

7.4. ניהול שוטף:

מנהל מערכות מידע יבצע פיקוח ומעקב שוטף אחר פעילויות מהותיות המבוצעות על ידי ספקים, אשר תכלול, בין היתר, התייחסות להיבטים הבאים:

- 7.4.1.** עמידת ספק השירות בהסכמי רמת שירות (SLA), בהסכמי רמת תפעול (OLA), בדרישות אבטחת מידע ובתנאי הסכם ההתקשרות;
- 7.4.2.** שינויים מהותיים באיתנות הפיננסית של ספק השירות.

7.5. דיווח:

- 7.5.1.** פעמיים בשנה, ידווח מנהל מערכות מידע לוועדת ההיגוי, אודות התקשרויות חדשות עם גורמי מיקור חוץ בתחום טכנולוגיות המידע ואבטחת מידע במערכות המידע, וכן אודות אירועים חריגים מול ספקי שירותים מהותיים.
- 7.5.2.** פעמיים בשנה, ידווח יו"ר וועדת ההיגוי להנהלת בנק הדואר אודות אירועים חריגים הנוגעים להתקשרויות עם גורמי מיקור חוץ בתחום טכנולוגיית המידע בכל הנוגע לשירותים הכספיים.

8. אספקת שירותים בתקשורת;

8.1. יעד

מזעור הסיכונים הכרוכים באספקת שירותי הבנק באמצעי תקשורת שונים.

8.2. קווים מנחים:

על הדירקטוריון לגבש מדיניות, אשר תבטיח כי שירותים בתקשורת, יינתנו על ידי הבנק באופן אשר יבטיח כי מידע רגיש אודות לקוחות לא ייחשף, וכי סיכונים הנובעים משימוש במנגנוני התקשורת מול הלקוח, ינוהלו באופן נאות. מדיניות זו תתייחס, לכל הפחות, לנושאים הבאים:

8.2.1. בהתאם לרישיון, הגדרת סוגי השירותים אותם ניתן לספק בתקשורת;

8.2.2. אמצעי זיהוי אישיים לכל מורשה גישה;

8.2.3. הקצאת הרשאות באופן אשר יבטיח כי כל משתמש יוכל לבצע אך ורק את הפעולות להן הוא מורשה;

8.2.4. קביעת עקרונות למדיניות ניהול סיסמאות לרבות התייחסות לאופן הנפקת סיסמאות, תוקף הסיסמאות וקריטריונים לחסימת חשבון הגישה של הלקוח.

8.2.5. בהתאם לסיכונים הכרוכים באופי השירותים, יש לבחון את הצורך במנגנוני מניעת הכחשה.

8.2.6. קביעת עקרונות למדיניות ניהול סיכונים בכל הנוגע לביצוע עסקאות בתחום השירותים הכספיים שלא פנים אל מול פנים (עסקאות מרחוק).

8.3. גיבוש תהליך:

8.3.1. תיעוד השירותים אותם מספק הבנק בתקשורת, בהתאם לאמור בסעיף 4.1.3.1 לעיל;

8.3.2. בהתאם לסיכונים הכרוכים באספקת כל אחד מהשירותים, תגדיר הנהלת בנק הדואר בקרות נדרשות, לרבות:

8.3.2.1. יישום אמצעי הצפנה של תווך התקשורת;

8.3.2.2. יישום מנגנוני אבטחת מידע שיבטיחו את זהות אתר האינטרנט כשייך לבנק;

8.3.2.3. יישום מנגנון ניתוק התקשורת, לאחר פרק זמן של אי-פעילות במערכת;

8.3.2.4. נקיטת אמצעי הגנה כגון: מניעת שמירת סיסמה בדפדפן, מניעת שמירת דפי אינטרנט בזיכרון "מטמון" וכדומה, אשר יבטיחו כי מידע רגיש לא יישמר על המחשב המשמש את הלקוח;

8.3.2.5. בכל כניסה של הלקוח לחשבון באמצעות שירותי בנקאות בתקשורת יוצגו בפניו באופן בולט פרטים על מועד ההתקשרות הקודמת.

8.3.3. במתן שירותים בתקשורת, מהווה סיסמת המשתמש את אחת הבקורות המשמעותיות ביותר. על כן, נדרשת הנהלת בנק הדואר לגבש תהליכים לניהול

הסימאות של חשבונות גישה לשירותים בנקאיים. תהליכים אלו, יכללו בין היתר את הבקורות הבאות:

- 8.3.3.1.** סימא תימסר ללקוח באופן אישי כשהיא חסויה;
- 8.3.3.2.** הלקוח יחויב להחליף סימא לאחר ההתקשרות הראשונית ולפחות אחת לחצי שנה;
- 8.3.3.3.** חשבון גישה של לקוח יחסם אוטומטית, במקרים הבאים:
 - א.** כאשר לא נעשה שימוש בסימא הראשונית תוך 30 יום מהנפקתה;
 - ב.** כאשר הלקוח או הבנק חושדים שנעשה שימוש בלתי מורשה בחשבון הגישה;
 - ג.** לאחר חמישה ניסיונות כניסה כושלים רצופים;
 - ד.** אי-שימוש בחשבון במשך חצי שנה;
 - ה.** שחרור חשבון חסום והקצאת סימא חדשה, תבוצע לאחר זיהוי הלקוח ובהתאם לסעיף 8.3.3.1 לעיל.

8.3.4. הנהלת בנק הדואר תגבש נוסח הסכם התקשרות עם הלקוחות למתן שירותי בנקאות בתקשורת. הסכם זה יכלול הצגה של סיכונים הקשורים בפעילויות אלה ותביא לידיעת הלקוחות את עקרונות האבטחה הננקטים על ידי הבנק. כמו כן, ימליץ הבנק על דרכי התגוננות מפני סיכונים אלה.

8.4. ניהול שוטף:

- 8.4.1.** מנהל אבטחת המידע בבנק הדואר, יהיה אחראי על ביצוע פעילות לאיתור ניסיונות התחזות לאתרי האינטרנט של הבנק;
- 8.4.2.** מנהל אבטחת המידע של הבנק יהיה אחראי על ניטור שוטף של פעילות וניסיונות גישה לאתרי הבנק, לשם איתור פעולות לא מורשות;
- 8.4.3.** בהמשך לאמור בסעיפים 3.4.5 - 3.4.8 לעיל, ביצוע מבדקי חדירה וסקרי סיכונים לאתרי הבנק ולמערכות טכנולוגיות אחרות, המשמשות לתקשורת מול לקוחות הבנק.

8.5. דיווח:

- 8.5.1.** אחת לחצי שנה לפחות, ידווח מנהל אבטחת המידע בבנק הדואר, לוועדת ההיגוי, אודות שינויים בהערכת הסיכונים וכן אודות אירועים חריגים הנוגעים לאספקת שירותים בתקשורת;
- 8.5.2.** אחת לחצי שנה לפחות, ידווח מנהל אבטחת המידע בבנק, לוועדת ההיגוי, אודות שינויים בהערכת הסיכונים וכן אודות אירועים חריגים הנוגעים לאספקת שירותים בתקשורת;

8.5.3. אחת לחצי שנה לפחות, ובתאום עם מנהל אבטחת מידע בבנק, ידווח מנהל סיכוני טכנולוגיית מידע, לוועדת ההיגוי, אודות שינויים בהערכת הסיכונים וכן אודות אירועים חריגים הנוגעים לאספקת שירותים בתקשורת;

8.5.4. שינויים מהותיים בהערכת הסיכונים, ואירועים משמעותיים אחרים ידווחו לדירקטוריון במסגרת הדיווח השנתי של מנהל הסיכונים, כאמור בסעיף 3.5 לעיל.

9. פרק ט': החלת ההוראה

9.1. תחולה

הוראה זו חלה על חברת דואר ישראל בע"מ בנותנה את השירותים כספיים לפי פרק 11 לחוק הדואר.

עם כניסתו לתוקף של היום הקובע כמשמעו בחוק הדואר (תיקון מספר 11) תשע"ב 2012, במקום חברת דואר ישראל בע"מ בנותנה את השירותים הכספיים יבוא, חברת בנק הדואר בע"מ.

9.2. תחילה

תחילתה של הוראה זו מיום 31 בדצמבר 2014.