

ניהול טכנולוגיית המידע

תוכן העניינים

357-2	כללי	פרק א'
357-2	1. מבוא	
357-2	2. תחולה	
357-3	פיקוח וניהול	פרק ב'
357-3	3. דירקטוריון	
357-3	4. הנהלה	
357-3	5. נהלים	
357-4	6. תיעוד, רישום ומעקב	
357-4	7. ביקורת פנימית	
357-5	סיכונים	פרק ג'
357-5	8. הערכת סיכונים	
357-6	אבטחת מידע	פרק ד'
357-6	9. מנהל אבטחת מידע	
357-6	10. אבטחת מידע	
357-7	11. סקר בטיחות וניסיונות חדירה מבוקרים	
357-7	12. בקרת גישה	
357-8	13. הצפנה	
357-8	14. קישוריות התאגיד הבנקאי לאינטרנט	
357-10	גיבוי והתאוששות	פרק ה'
357-10	15. דיון בהנהלה	
357-10	16. הסדרי גיבוי והתאוששות	
357-11	מיקור חוץ	פרק ו'
357-11	17. מיקור חוץ	
357-11	18. הסכם התקשרות	
357-12	שירותי בנקאות בתקשורת	פרק ז'
357-12	19. הגדרות	
357-13	20. הסכם התקשרות למתן שירותי בנקאות בתקשורת	
357-14	21. גילוי נאות	
357-14	22. אמצעי זיהוי והרשאות	
357-15	23. ניהול סיסמאות	
357-15	24. אמצעי בקרה	
357-16	25. עסקאות בתקשורת לטובת צד שלישי	
357-16	26. רשימת מוטבים	
357-17	27. דואר אלקטרוני	
357-18	28. ריכוז מידע	
357-19	שונות	פרק ח'
357-19	29. בנק חוץ	
357-19	30. פעולות הטעונות הסכמה ופעולות הטעונות דיווח	

פרק א': כללי

מבוא

1. (א) מערך טכנולוגיית המידע הוא מרכיב מרכזי בתפעול ובניהול התקין של תאגיד בנקאי, לאור היותו של המידע, על כל היבטיו והשלכותיו, בעל השפעה מכרעת על יציבות התאגיד הבנקאי והתפתחותו.
- (ב) בשל גורמים אלו על הנהלת תאגיד בנקאי לייחס את החשיבות הראויה, הן בהיררכיה הניהולית והן במשאבים הכספיים ומשאבי האנוש הנחוצים, לניהול תקין של מערך טכנולוגיית המידע.
- (ג) מבלי לפגוע בכלליות האמור לעיל, נקבעה הוראה זו הכוללת הנחיות פרטניות וכלליות.
- (ד) הוראה זו תואמת את העקרונות בתחום הבנקאות האלקטרונית, שפירסמה הועדה הבינלאומית לפיקוח על הבנקים (ועדת באזל) ביולי 2003.

תחולה

2. הוראה זו תחול על תאגידים בנקאיים, וכן על תאגידים כאמור בסעיפים 11(א)(3), 11(א)(3)ב) ו-11(ב) לחוק הבנקאות (רישוי), התשמ"א-1981 שהואגדו בישראל (להלן: תאגיד בנקאי).

פרק ב': פיקוח וניהול

דירקטוריון

3. (א) דירקטוריון של תאגיד בנקאי יקיים דיון תקופתי ויקבע את מדיניות ניהול טכנולוגיית המידע של התאגיד הבנקאי, בהתאם לאמור בסעיף 6(ד) להוראת ניהול בנקאי תקין מס' 301 (דירקטוריון).
- (ב) מדיניות ניהול טכנולוגיית המידע תכלול, בין היתר, התייחסות ל:
- (1) אבטחת מידע;
 - (2) עקרונות גיבוי והתאוששות במצבים של תקלות ואסונות;
 - (3) מיקור חוץ;
 - (4) מדיניות פיתוח, לרבות על-ידי משתמשי קצה;
 - (5) שימוש בטכנולוגיות חדשות במסגרת הבנקאות בתקשורת.

הנהלה

4. (א) הנהלת תאגיד בנקאי תמנה מנהל אחד שיהיה חבר הנהלה או כפוף למנכ"ל, אשר יישא באחריות למכלול נושאי טכנולוגיית המידע (להלן: מנהל טכנולוגיית המידע). מנהל זה יהיה בעל הכשרה מקצועית מתאימה וניסיון מוכח בתחום טכנולוגיית המידע וניהולו.
- (א1) על אף האמור בסעיף קטן (א), המפקח על הבנקים רשאי להתיר, במקרים חריגים, למנהל טכנולוגיית המידע בתאגיד הבנקאי לשמש מנהל טכנולוגיית המידע גם בתאגידים בנקאיים הנשלטים על ידי אותו תאגיד בנקאי או בתאגידים כמפורט בסעיפים 11(א)(א3), 11(א)(ב3), ו-11(ב) לחוק הבנקאות (רישוי).
- (ב) הנהלת תאגיד בנקאי תמנה מנהל אבטחת מידע, כמפורט בסעיף 9.
- (ג) הנהלת תאגיד בנקאי תקיים דיון שנתי ביישום מדיניות ניהול טכנולוגיית המידע ותקצובה, ותקבל את ההחלטות הנגזרות, תוך הבחנה בין נושאים רלבנטיים לטווח הקצר לבין נושאים רלבנטיים לטווח הארוך.
- (ד) הנהלת תאגיד בנקאי תייחד דיון שנתי ליישום מדיניות אבטחת המידע על כל היבטיה.
- (ה) בקביעת המבנה הארגוני של היחידה המופקדת על ניהול טכנולוגיית המידע בתאגיד הבנקאי, ובהגדרת התפקידים של עובדי יחידה זו, תקיים הנהלת התאגיד הבנקאי הפרדת תפקידים וסמכויות נאותה.
- (ו) הנהלת תאגיד בנקאי תגדיר את סוגי הפעילויות והאירועים שלגביהם יש לספק התראה להנהלה ולגורמים מוסמכים אחרים, לרבות אלו המחייבים התראה בזמן אמת.

נהלים

5. תאגיד בנקאי יקבע נהלים מפורטים לכל שלב ולכל תהליך המטפלים בניהול, תפעול, אבטחה, גיבוי, שרידות ובקרה של טכנולוגיית המידע, ויקיים בקרה נאותה על ביצועם. נהלים אלה יעודכנו באופן שוטף בהתאם לשינויים החלים הן בסביבה העסקית הרלבנטית והן בסביבה הטכנולוגית.

תיעוד, רישום ומעקב

6. (א) תאגיד בנקאי יקיים תיעוד מתאים ועדכני למערך טכנולוגיית המידע שלו.
- (ב) (1) תאגיד בנקאי יקיים נתיב ביקורת שיתבסס על רישום ממוכן (log) של עצם הגישה ושל פעולות ושאליות המבוצעות במערכות המידע של התאגיד הבנקאי, אשר יכלול, בין היתר, את זיהוי מורשה הגישה, המקום, הזמן וכן פרטים על נושא הגישה.
- (2) על אף האמור בפסקה (1) לעיל, לגבי שאילתות של עובדי התאגיד הבנקאי יקיים התאגיד הבנקאי נתיב ביקורת על פי שיקול דעתו, תוך התבססות על הערכת הסיכונים.
- (3) תאגיד בנקאי יקבע את פרק הזמן לשמירת הרישומים כאמור בפסקה (1), ובלבד שפרק הזמן לשמירת הרישומים לא יקטן מ- 60 יום לרישומי שאילתות ו-6 חודשים לרישומי פעולות.
- (ג) תאגיד בנקאי יידע את לקוחותיו ואת עובדיו לגבי עצם קיומם של הליכי שמירה של פעולותיהם.
- (ד) בכפוף לאמור בסעיף 4(ו), מערכות ניהול הרישומים תספקנה לגורמים המוסמכים לכך, התראות על פעילויות חיצוניות בלתי מורשות וכן על פעילויות חריגות של המשתמשים לסוגיהם.

ביקורת פנימית

7. (א) תאגיד בנקאי יכלול, במסגרת הביקורת הפנימית שלו, יחידה ארגונית לביקורת טכנולוגיית המידע שלו. האחראי על הביקורת הפנימית בתחום טכנולוגיית המידע יהיה בעל הכשרה מקצועית וניסיון רלבנטיים לביצוע הביקורת בתחום זה.
- (ב) תאגיד בנקאי יעמיד לרשות הביקורת הפנימית את הכלים הדרושים לביצוע ביקורת ובקרה בסביבת מערך טכנולוגיית המידע.
- (ג) בכל מקרה בו נעשה שימוש במיקור חוץ של ביקורת פנימית בתחום טכנולוגיית המידע, יש לשמור על יכולת ההערכה בידי הביקורת הפנימית של התאגיד הבנקאי.

פרק ג': סיכונים

הערכת סיכונים

8. (א) הנהלת תאגיד בנקאי תבצע הערכת סיכונים (Risk Assessment) של מערך טכנולוגיית המידע. על הערכת הסיכונים להתייחס למכלול הסיכונים הפוטנציאליים הקשורים בניהול מערך טכנולוגיית המידע, כגון:
- משתמשי המערכת הפנימיים והחיצוניים לתאגיד הבנקאי;
 - סביבת המערכת;
 - פעילות המערכת והשלכותיה על עסקי התאגיד;
 - רגישות המידע;
 - מיקור חוץ.
- (ב) תהליך הערכת הסיכונים יהיה מתמשך, והערכת הסיכונים תתעדכן בהתאם לשינויים בגורמי הסיכון השונים.
- (ג) בהתאם להערכת הסיכונים על התאגיד הבנקאי לנקוט באמצעים הנדרשים למזעור אפשרות פגיעה במערך טכנולוגיית המידע על כל חלקיו, ומזעור נזק פוטנציאלי.

פרק ד': אבטחת מידע**מנהל אבטחת מידע**

9. (א) (1) מנהל אבטחת מידע יהיה כפוף לחבר הנהלה של התאגיד הבנקאי.
- (א1) על אף האמור בסעיף קטן (1), המפקח על הבנקים רשאי להתיר, במקרים חריגים, למנהל אבטחת המידע בתאגיד הבנקאי לשמש מנהל אבטחת המידע גם בתאגידים בנקאיים הנשלטים על ידי אותו תאגיד בנקאי או בתאגידים כמפורט בסעיפים 11(א)(א3), 11(א)(ב3), ו-11(ב) לחוק הבנקאות (רישוי).
- (2) מנהל אבטחת מידע לא יעסוק בתפקידים ביצועיים אשר עלולים לגרום ניגוד עניינים, ובכלל זה לא ישמש כמנהל טכנולוגיית המידע.
- (3) הנהלת תאגיד בנקאי תקבע את תחומי אחריותו של מנהל אבטחת המידע ואת הנושאים שהחלטות לגביהם טעונות התייחסותו. תחומי אחריותו יכללו, בין היתר:
- אחריות כוללת ליישום מדיניות אבטחת המידע בתאגיד הבנקאי;
 - פיתוח ומעקב של יישום תוכניות אבטחת המידע בתאגיד הבנקאי ובחינה של אפקטיביות מערכת אבטחת המידע;
 - טיפול באירועים חריגים בתחום אבטחת המידע.
- (4) הנהלת תאגיד בנקאי תעמיד לרשות מנהל אבטחת המידע את המשאבים הדרושים למילוי תפקידו.
- (ב) מנהל אבטחת מידע יהיה בעל הכשרה מקצועית וניסיון רלבנטיים בתחום עיסוקו.

אבטחת מידע

10. (א) הנהלת תאגיד בנקאי תרכז את עקרונות אבטחת המידע במסמך כתוב, אשר יובא לאישור הדירקטוריון. מסמך זה יעודכן אחת לתקופה.
- (ב) תאגיד בנקאי יישם אמצעי אבטחה - פיזית ולוגית, למניעה, גילוי, תיקון ותיעוד של חשיפות במערך טכנולוגיית המידע ודיווח עליהם, בהתאם להערכת הסיכונים ותוך התייחסות גם להיבטים הבאים:
- (1) זיהוי ואימות (Identification & Authentication);
 - (2) סודיות ופרטיות (Privacy);
 - (3) שלמות ומהימנות של הנתונים (Integrity);
 - (4) מניעת הכחשה (Non Repudiation).
- (ג) תאגיד בנקאי ינהל מעקב שוטף אחר ההתפתחויות הטכנולוגיות, ויתאים את רמת האבטחה ובקרת הגישה למערכותיו על פי השינויים ברמת הסיכונים הנגזרים משינויים טכנולוגיים אלו.
- (ד) תאגיד בנקאי יפעל להפרדת סביבת הייצור (Production) מסביבת הפיתוח והניסוי (Test).

סקר בטיחות וניסיונות חדירה מבוקרים

11. (א) אחת לתקופה, בהתאם להערכת הסיכונים, ייזום מנהל אבטחת המידע סקר בטיחות של מערך טכנולוגיית המידע של התאגיד הבנקאי (להלן: הסקר). בסקר שיבוצע תוערך האפקטיביות של אמצעי ההגנה, בהתייחס להערכת הסיכונים, ויוצעו דרכים לתיקון הליקויים שיימצאו.
- (2) לגבי מערכות שהוגדרו על-ידי התאגיד הבנקאי כבעלות סיכון גבוה, לרבות מערכות בנקאות בתקשורת, יש לערוך סקר במתכונת כאמור בפסקה (1) לעיל לפני הטמעת שינויים משמעותיים במערכות אלו, כאשר חלו שינויים משמעותיים בסביבה הטכנולוגית בה המערכות פועלות, וכן לקראת הכנסתן לשימוש של מערכות חדשות כאמור, ולפחות אחת ל-18 חודשים.
- (3) תוצאות הסקר יכללו דוח מפורט על הממצאים וההמלצות, ותמצית ניהולית שתציג את עיקרי הדברים.
- (ב) מנהל אבטחת מידע ייזום ניסיונות חדירה מבוקרים למערך טכנולוגיית המידע של התאגיד הבנקאי לבחינת עמידותו בפני סיכונים פנימיים וחיצוניים. פעולה זו תיעשה בתדירות ההולמת את הסיכונים הספציפיים של המערכות השונות, בהתאם להערכת הסיכונים.
- (ג) (1) סקר הבטיחות וניסיונות החדירה המבוקרים, כאמור לעיל, ייערכו על ידי גורמים מקצועיים, עצמאיים, בלתי תלויים, חיצוניים לתאגיד הבנקאי, תוך מניעת ניגודי עניינים ונקיטת אמצעי הזהירות המתחייבים.
- (2) הנהלת תאגיד בנקאי תשלים את דיוניה בממצאי סקר הבטיחות וניסיונות החדירה המבוקרים והשלכותיהם, ותקבל את ההחלטות המתחייבות, לרבות קביעת לוח זמנים ליישומן, תוך פרק זמן סביר לאחר מועד תחילת ביצועם.
- (ד) ממצאים מהותיים שעלו בסקר הבטיחות וניסיונות החדירה המבוקרים יובאו לידיעת הדירקטוריון או ועדה דירקטוריונית מתאימה.

בקרת גישה

12. (א) (1) תאגיד בנקאי יבצע זיהוי אישי חד-ערכי של כל גורם בעל גישה למערכת מידע (להלן: מורשה גישה) כתנאי מוקדם למתן הגישה.
- (2) על אף האמור בפסקה (1) לעיל, במקרים חריגים של ספקים ועובדים בהם לא ניתן לקיים את האמור לעיל, יישם התאגיד הבנקאי אמצעים חלופיים מתאימים.
- (ב) (1) תאגיד בנקאי יקבע כללים וכלים לזיהוי ולמתן הרשאות לגורמים שונים לרכיבי טכנולוגיית המידע. כללים אלו יביאו בחשבון את רמות הסיכון הנגזרות מטווח האחריות והסמכות של המשתמשים (על-פי סיווג לקבוצות), מהיישום עצמו, מרגישות המידע ומשאר רכיבי טכנולוגיית המידע.
- (2) הסיווג לקבוצות משתמשים יתייחס לגורמים הפנימיים בתאגיד הבנקאי ולגורמים החיצוניים (לרבות לקוחות, ספקים וכו').
- (3) תאגיד בנקאי יפעיל כלים לניהול ולבקרה של מערכת ההרשאות.
- (4) אמצעי הגישה למערכות המידע יהיו בטכניקות מקובלות לענין זה.

- (ג) (1) לצורך בקרת גישה למערכות מידע שהוערכו כבעלות סיכון גבוה, ובכל מקרה של גישה מרחוק למערך טכנולוגיית המידע של התאגיד הבנקאי על ידי עובדים, ספקים ונותני שירותים, ישתמש התאגיד הבנקאי בטכנולוגיה המשלבת זיהוי ואימות של המשתמש, סודיות ושלמות הנתונים ומניעת הכחשה.
- (2) על אף האמור בפסקה (1) לעיל, רשאי תאגיד בנקאי להשתמש בטכנולוגיה חלופית במקרים הבאים:
- במערכות בסיכון גבוה שלא באמצעות גישה מרחוק, על פי שיקול דעתו של התאגיד הבנקאי, שתועד בכתב;
 - בגישה מרחוק של ספקים ונותני שירותים, כאשר שימוש בטכנולוגיה כאמור אינו אפשרי מסיבות שאינן תלויות בתאגיד הבנקאי.
- (ד) תאגיד בנקאי יקבע קריטריונים להפעלת מנגנון ניתוק התקשורת (Time-out) לאחר פרק זמן שבו לא היתה פעילות מצד מורשה הגישה. פרק הזמן ייקבע תוך התחשבות בהערכת הסיכונים.

הצפנה

13. תאגיד בנקאי יבחן את הצורך בהצפנה של נתונים, לרבות בתווך התקשורת, במערכות שהוגדרו בהתאם להערכת הסיכונים כבעלות סיכון גבוה, ובלבד שבמקרים הבאים תתקיים הצפנה:
- (א) בנקאות בתקשורת באמצעות האינטרנט, לרבות באמצעות דואר אלקטרוני;
- (א1) על אף האמור בסעיף קטן (א), לא תידרש הצפנה בהעברת מידע בדואר אלקטרוני בנוגע לחשבון של בנק הפועל והמפקח מחוץ לגבולות ישראל (להלן: בנק זר), בהתקיים התנאים הבאים:
- (1) ניתנה הודעה לבנק הזר כי המידע מועבר ללא הצפנה;
 - (2) הונהגו בקרות מתאימות ע"י התאגיד הבנקאי לעניין זה;
 - (3) פנה התאגיד הבנקאי למפקח וקיבל את אישורו.
- (ב) גישה מרחוק למחשב התאגיד הבנקאי, בכפוף לאמור בסעיף 12(ג).
- (ג) סיסמאות של מורשי גישה.

קישוריות התאגיד הבנקאי לאינטרנט

14. (א) תאגיד בנקאי ינקוט באמצעים לאיתור התחזות לאתר האינטרנט שלו, ויספק ללקוח כלים מתאימים לוודא את זהות האתר של התאגיד הבנקאי.
- (ב) קישוריות התאגיד הבנקאי לאינטרנט תיעשה במקרים הבאים בלבד:
- (1) קישוריות עובדים לאינטרנט, כמפורט בסעיפים קטנים (ג) ו-(ד);
 - (2) מתן שירותי בנקאות בתקשורת, כמפורט בפרק ז';
 - (3) שימוש אחר שאושר מראש על-ידי המפקח, כאמור בסעיף 30(א).
- (ג) הנהלת תאגיד בנקאי תקבע את השימושים המותרים לעובדי התאגיד הבנקאי באמצעות קישוריות לאינטרנט, על פי הערכת סיכונים ותוך נקיטת אמצעי בקרה נאותים ובכפוף לאמור בסעיף קטן (ד).

- (ד) קישוריות עובדי התאגיד הבנקאי לאינטרנט מתחנות עבודה תתאפשר בהתקיים אחד מאלה:
- (1) תחנת העבודה קשורה אך ורק לאינטרנט או לרשת שקשורה אך ורק לאינטרנט (Stand Alone) ושאינ עליה יישומים בנקאיים או מידע רגיש;
- (2) הקישוריות לאינטרנט תיעשה באמצעות שרת נפרד של התאגיד הבנקאי, ותבוקר באופן שוטף על ידי האמצעים האמורים בסעיף קטן (ה). בתצורה זו, הקישוריות לאינטרנט תבוצע לצורכי גלישה ודואר אלקטרוני בלבד;
- (ה) בהתאם לאמור בסעיף 10(ג), קישוריות של רשת התאגיד הבנקאי לאינטרנט תאובטח לפחות על-ידי אנטי וירוס, מסנני תוכן (Content-Filtering), מערכת לאיתור ניסיונות חדירה (IDS) ו-Firewall.
- (ו) התאגיד הבנקאי יישם, על פי הערכת הסיכונים, אמצעים ממוכנים לבקרת אפליקציה ולסריקת חולשות המערכת.
- (ז) האמור בסעיפים קטנים (ה) ו- (ו) יחול על כל אתרי התאגיד הבנקאי, לרבות האתר השיווקי.

פרק ה': גיבוי והתאוששות**דיון בהנהלה**

15. (א) אחת לתקופה תקיים הנהלת תאגיד בנקאי דיון בעקרונות הגיבוי וההתאוששות ותקבל החלטות בתחום זה, תוך התייחסות מפורטת להערכת הסיכונים ולעניינים הבאים:
- (1) הגדרת מצבי תקלות (לרבות אצל ספקי התאגיד הבנקאי) ואסונות (לרבות אסונות טבע, שריפות, מלחמה ושעת חירום) עבור מכלול היחידות הארגוניות, והשלכותיהם על המשך הפעילות של התאגיד הבנקאי;
 - (2) קביעת התהליכים העסקיים החיוניים גם במצבי תקלות ואסונות, מערכות המידע הרלבנטיות לתפעולם ואופן תפעולן של מערכות אלו במצבים כאמור;
 - (3) רכיבי התוכנה, החומרה והתקשורת השונים;
 - (4) היבטי הגיבוי וההתאוששות, לרבות התייחסות לגיבוי שוטף, משך הגיבוי, תדירות הגיבוי, מדיית הגיבוי, זמני השבתה מרביים, ותהליך החזרה לשגרת העבודה;
 - (5) הסתמכות על גורמי חוץ בעת קיומן של הפרעות לפעולה סדירה של מערכות המידע, וזמן ההתאוששות הנחוץ לתאגיד הבנקאי להחזרת מערכות המידע לפעולה סדירה.
- (ב) במסגרת הדיון יוחלט על הסדרי הגיבוי השוטף (לרבות גיבוי לכוח אדם ולתיעוד) ועל השקעות במתקני גיבוי ובהסדרי גיבוי אחרים עבור מערכות מהותיות שנקבעו על פי האמור בסעיף קטן (א)(2) לעיל.

הסדרי גיבוי והתאוששות

16. (א) (1) תאגיד בנקאי יקיים תכנית מפורטת להפעלת מערך טכנולוגיית המידע שלו במקרים של תקלות ואסונות (להלן: תכנית התאוששות מאסון), כאמור בסעיף 15.
- (2) תאגיד בנקאי יבחן ויעדכן את תכנית ההתאוששות מאסון על-פי השינויים שחלו בתקופה שחלפה מהעדכון הקודם (לרבות שינויים במערך החירום ובהערכת הסיכונים) לפחות אחת לשנתיים וכן בעת ביצוע שינוי מהותי.
- (ב) לפחות אחת לשנתיים וכן בעת ביצוע שינוי מהותי במערך החירום, יקיים תאגיד בנקאי ניסוי של כל הסדרי הגיבוי וההתאוששות שלו.
- (ג) אחסון גיבויי ציוד, תוכנה ומידע חיוניים יהיה במקום מרוחק ממקום אחסון המקור, כך שאירועים כאסון טבע, מלחמה ודומיהם לא יפגעו בו-זמנית בציוד, בתוכנה ובמידע המקוריים ובגיבוי, ולא ימנעו שימוש בהם.
- (ד) תאגיד בנקאי ינקוט באמצעים שיבטיחו אפשרות שחזור מידע מעותקי גיבוי, לרבות מידע שנשמר באמצעים שחדלו לשמש אותו.

פרק ו': מיקור חוץ**מיקור חוץ**

17. (א) תאגיד בנקאי רשאי לבצע פעילויות ניהול, עיבוד ואחסון של המידע שלו או פיתוח מערכות, לרבות שירותי יעוץ, ידע ושירותים אחרים, על-ידי גורמים מחוץ לתאגיד הבנקאי (להלן: גורמים חיצוניים).
- (ב) על אף האמור בסעיף קטן (א), מיקור חוץ כמפורט להלן טעון הסכמה של המפקח, כאמור בסעיף 30(א):
- (1) מיקור חוץ של מערכות הליבה (Core Systems);
 - (2) אחסון מידע מכל סוג שהוא לגבי לקוחות התאגיד הבנקאי במערכות שאינן בשליטתו הבלעדית;
 - (3) סעיף זה אינו חל על שירותי מיקור חוץ שמקבל תאגיד בנקאי כאמור בסעיף 11(א) לחוק הבנקאות (רישוי), התשמ"א - 1981, מתאגיד בנקאי השולט בו או מתאגיד עזר שבשליטת התאגיד הבנקאי השולט בו.
 - (ג) אין לבצע מיקור חוץ של שירותי ריכוז מידע (Account Aggregation).
 - (ד) במיקור חוץ מהותי, תאגיד בנקאי יוודא את מהימנותו ואת חוסנו הכלכלי של נותן השירותים, ויבחן מראש את התאמת כישוריו ואת יכולתו לבצע את המטלות.

הסכם התקשרות

18. (א) התקשרות לצורך מיקור חוץ תיעשה בהסכם כתוב.
- (ב) במיקור חוץ מהותי, הסכם ההתקשרות יתייחס מפורשות לפחות לנושאים הבאים:
- (1) הגדרת תחומי אחריות של כל אחד מהצדדים להסכם, לרבות קבלני משנה;
 - (2) הסכם רמת השירות (SLA);
 - (3) חובת הסודיות, אבטחת מידע ומצבי חירום;
 - (4) הסדרים להפסקת ההסכם וליישוב מחלוקות. בהקשר זה יתייחס ההסכם גם להסדרים שיאפשרו לתאגיד הבנקאי לתפעל ולתחזק את פעילות מיקור החוץ במקרים בהם הגורם החיצוני חדל מלספק את השירות (כגון על-ידי החזקת תוכניות מקור אצל נאמן);
 - (5) פעילות הגורם החיצוני עבור התאגיד הבנקאי יהיו ניתנות לביקורת מטעמו.
- (ג) אין בהוראת סעיף זה בכדי לגרוע מאחריותו של התאגיד הבנקאי לכל פעולה שנעשת מטעמו על ידי גורמים חיצוניים.

פרק ז': שירותי בנקאות בתקשורת

הגדרות

19. (א) "בנקאות בתקשורת" - אחזור מידע על חשבונותיו של לקוח התאגיד הבנקאי או ביצוע פעולות או מתן הוראות לביצוע פעולות ביוזמת לקוח התאגיד הבנקאי, באמצעות מערכות תקשורת המקושרות למחשב התאגיד הבנקאי והעושות שימוש ברשת תקשורת (כגון: טלפוניה, אינטרנט, סלולרית) או שילוב בין רשתות תקשורת, למעט פעולות שהוראת ניהול בנקאי תקין מספר 435 (הוראות טלפוניות) חלה עליהן.

- (1) (ב) רמות השירות של שירותי בנקאות בתקשורת מוגדרות להלן:
- (א) "רמת שירות (1)" - העברת מידע מן התאגיד הבנקאי ללקוח על חשבונותיו (תנועות ויתרות);
- (ב) "רמת שירות (2)" - עסקאות ופעולות בחשבונות של הלקוח בתאגיד הבנקאי (כגון: העברה לפיקדונות קבועים, רכישת ניירות ערך, העברה מחשבון לחשבון, הזמנת פנקסי שיקים וכיו"ב);
- (ג) "רמת שירות (3)" - עסקאות לטובת חשבונות שנקבעו על-ידי הלקוח מראש באמצעות רשימת מוטבים;
- (ד) "רמת שירות (4)" - עסקאות לטובת חשבונות אשר אינם כלולים באחת מרמות השירות לעיל.

מובהר בזה, כי לענין הבקורות ואבטחת המידע, כל רמת שירות בפסקאות (ב) עד (ד) לעיל כוללת את רמות השירות שקדמו לה.

- (2) עדכון פרטים אישיים בערוצי בנקאות בתקשורת של לקוח ייעשה בתנאים הבאים:
- (א) עדכון פרטים אישיים לעניין בקורות ואבטחת המידע, יחשב כרמת שירות (2), ויחול רק על פרטים אישיים המשמשים להעברת מידע מן התאגיד הבנקאי ללקוח על חשבונותיו (כאמור בסעיף 19(ב)(1)(א)), כגון, מספר טלפון סלולרי ודואר אלקטרוני;
- (ב) לא ניתן יהיה לשנות שם, מספר תעודת זהות וכתובת פיסית של הלקוח;
- (ג) הפרטים האישיים המעודכנים לא ישמשו לצורך זיהוי ובקרה של הלקוח;
- (ד) התאגיד הבנקאי יקיים בקרה שהגורם שעדכן את פרטי הלקוח הוא הלקוח עצמו;
- (ה) פרטי המידע שניתן יהיה לעדכן ייקבעו לאחר קבלת החלטה מנומקת על ידי התאגיד הבנקאי על פי הערכת סיכונים.
- (ו) על אף האמור בסעיף קטן (א), אם הלקוח צורף לרמת שירות שאינה גבוהה מרמת שירות (1), יחשב עדכון פרטים כרמת שירות (1).

הסכם התקשרות למתן שירותי בנקאות בתקשורת

20. (א) הסכם ההתקשרות בין התאגיד הבנקאי לבין הלקוח למתן שירותי בנקאות בתקשורת ייחתם בסניף, ויאפשר ללקוח לבחור בנפרד כל רמת שירות וכל ערוץ תקשורת המוצע על-ידי התאגיד הבנקאי אשר הלקוח מבקש לקבלו. במעמד הסכם ההתקשרות יימסרו ללקוח אמצעי זיהוי ראשוניים לצורך התחברות לשירותי בנקאות בתקשורת.
- (ב) על אף האמור בסעיף קטן (א) לעיל, ניתן לכרות הסכם בערוצי בנקאות בתקשורת (להלן: הסכם מקוון), ובלבד שיתמלאו לגביו התנאים הבאים:
- (1) (א) ההסכם המקוון יאפשר שירותים ברמת שירות (1) בלבד, לרבות ריכוז מידע (כאמור בסעיף 28); או
 - (ב) ההסכם המקוון יאפשר פעילות במערכת סגורה כהגדרתה בסעיף 1 להוראת ניהול בנקאי תקין מספר 417 בנושא – "פעילות תאגיד בנקאי במערכת סגורה";
 - (2) חברת כרטיסי אשראי רשאית, בנוסף לאמור בפיסקה (1) לעיל, לכלול בהסכם מקוון גם מתן אשראי, ובלבד שהאשראי לא יחרוג ממסגרת האשראי הלא מנוצלת של הלקוח;
 - (3) ההסכם המקוון יאפשר ללקוח לבחור בנפרד כל ערוץ תקשורת המוצע על ידי התאגיד הבנקאי;
 - (4) נוסח ההסכם המקוון יוצג במלואו על גבי המסך בצורה בהירה וקריאה, וניתן יהיה להדפיסו.
- (א4) הסכם מקוון, כאמור בסעיף קטן 1(א), יכול להיכרת גם באמצעות הוראה טלפונית. בהסכם מקוון שבוצע בהוראה טלפונית, לרבות באמצעות מענה טלפוני ממוחשב, יישלח ההסכם המקוון ללקוח, ויתקיימו מלבד יתר הוראות סעיף 20(ב), גם התנאים הבאים:
- (1) הפעלת אמצעי המאפשר לוודא שהלקוח ראה את ההסכם;
 - (2) הסכמה מפורשת של הלקוח להסכם;
 - (3) הקלטת השיחה הטלפונית או רישום ממוכן כאמור בסעיף 6(ב) לעיל.
- (ב4) תנאי ההסכם המקוון לא ירעו את מצב הלקוח ביחס להסכמים אחרים עליהם חתם הלקוח בעבר.
- (5) הודעה על כריתת הסכם מקוון תישלח ללקוח בדואר לא יאוחר משבוע ימים ממועד כריתת ההסכם, לפי הכתובת הרשומה בתאגיד הבנקאי;
 - (6) זיהוי הלקוח לצורך ההסכם המקוון יתבסס לפחות על שני פריטי זיהוי אשר אינם נשמרים בדרך כלל יחד;
 - (7) תאגיד בנקאי ימסור, לפי הענין, את אמצעי הזיהוי הראשון (כגון: קוד המשתמש) ואת הסיסמה הראשונית, ללקוח שטרם נמסרו לו פריטים אלו לצורך קבלת שירותי בנקאות בתקשורת, בסניף או בשתי דרכים שונות (כגון: האחד בדואר, לפי הכתובת הרשומה בתאגיד הבנקאי, והשני באינטרנט);
 - (8) אין באמור בסעיף זה כדי לגרוע מהאמור בכללי הבנקאות (שירות ללקוח) (גילוי נאות ומסירת מסמכים), התשנ"ב - 1992 (להלן: כללי גילוי נאות).
- (ג) על אף האמור בסעיפים (ב)1, (ב)6, ו-7(ב) לעיל, רשאי תאגיד בנקאי לכרות הסכם מקוון לכל רמת שירות, ובלבד שיתקיימו התנאים הבאים:
- (1) הלקוח חתם בעבר בסניף על הסכם למתן שירותי בנקאות בתקשורת בערוץ אחר;

- (2) רמת השירות שאליה מצטרף הלקוח לא תורחב מעבר לרמת השירות הקיימת בערוץ אליו צורף הלקוח בעבר ;
- (3) החתימה על הסכם מקוון תיעשה באותו ערוץ שאליה צורף הלקוח בעבר בסניף, ובאותם אמצעי זיהוי ;
- (4) הערוץ אליו צורף הלקוח בעבר, ושבאמצעותו נחתם ההסכם המקוון, אינו מכשיר בנק אוטומטי (ATM) או עמדת שירות.
- (ג) בהסכם מקוון יתאפשר ללקוח לגרוע כל רמת שירות אשר נכרתה בהסכם מסוג זה.
- (ד) תאגיד בנקאי יודיע למפקח בכתב על כל ערוץ חדש שניתן לקבל באמצעות הסכם מקוון כאמור בסעיפים קטנים (ב) ו-(ג) לעיל.
- (ה) תאגיד בנקאי לא יציע ללקוחותיו שירותי בנקאות בתקשורת בשיטות או באמצעים אשר נועדו למנוע מהלקוח לקבל שירותים דומים מתאגידים בנקאיים או מספקי שירות ומידע אחרים.
- (ו) המפקח על הבנקים רשאי, מטעמים מיוחדים שיירשמו, לתת לתאגיד בנקאי אישור לפעול בדרך חלופית לאמור בסעיף זה.

גילוי נאות

21. תאגיד בנקאי יציג בפני לקוחותיו את התנאים, הסייגים והסיכונים הקשורים לשימוש בשירותי בנקאות בתקשורת הניתנים על-ידו, יביא לידיעת לקוחותיו את עקרונות האבטחה הננקטים על-ידו על-מנת למזער סיכונים אלה, וימליץ בפני לקוחותיו על דרכי התגוננות מפני סיכונים אלה. כמו כן יודיע התאגיד הבנקאי ללקוחותיו כי אין באמור לעיל כדי לגרוע מאחריותו של מי מהצדדים.

אמצעי זיהוי והרשאות

22. (א) בהתאם לאמור בסעיף 12(א), תאגיד בנקאי יקבע אמצעי זיהוי אישיים לכל לקוח מורשה גישה בחשבון.

(ב) בנוסף לאמור בסעיף (א) לעיל, הזדהות במכשירי בנק אוטומטיים (ATM) ועמדות שירות תיעשה לפחות באמצעות שניים מתוך שלושת הפריטים כדלהלן :

(1) פריט הידוע למשתמש (Something you know) ;

(2) פריט הנמצא ברשות המשתמש (Something you have) ;

(3) פריט שהוא המשתמש (Something you are).

כאשר ההזדהות נעשית באמצעות אמצעי זיהוי כאמור בפסקה (2) לעיל, על התאגיד הבנקאי ליישם טכנולוגיה שתמנע, ככל שניתן, את האפשרות לשחזר את הנתונים הכלולים בפריט על ידי גורמים בלתי מורשים.

(ג) (1) הרשאותיו של הלקוח לביצוע פעולות ואחזור מידע במסגרת שירותי בנקאות בתקשורת, לא תחרוגנה מההרשאות שיש ללקוח בחשבון.

(2) על אף האמור בסעיף קטן (1), רשאי תאגיד בנקאי להגיע להסכמה עם לקוח שהינו תאגיד, כי מי שהורשה על ידי הלקוח יפעל לבדו במסגרת שירותי בנקאות בתקשורת, גם במקום בהן ההרשאות לפעול בחשבון שלא במסגרת שירותי בנקאות בתקשורת

הינן שונות, ובלבד שהתאגיד הבנקאי הגיע להסכמה זו עם הלקוח בכתב, ותוך קבלת אישור מאומת על החלטה המאפשרת זאת שהתקבלה ע"י האורגן המוסמך בתאגיד לעניין זה.

ניהול סיסמאות

23. (א) בניהול סיסמאות לזיהוי ואימות לקוחותיו יביא תאגיד בנקאי בחשבון את רמת השירות ורמת הסיכון של המערכת.

(ב) (1) הסיסמה הראשונית תימסר ללקוח באופן אישי כשהיא חסויה.

(2) הסיסמה הראשונית תימסר ללקוח בסניף, או באמצעות ערוץ תקשורת אחר אליו צורף הלקוח קודם לכן.

(3) לענין סעיף זה, "סיסמה ראשונית" - לרבות סיסמא הניתנת ללקוח בעת שחרור סיסמה.

(4) האמור בפסקה (2) לא יחול על הסכם מקוון, כאמור בסעיף 20(ב).

(ג) תאגיד בנקאי ייזום החלפת הסיסמה על ידי הלקוח במקרים הבאים:

(1) מיד לאחר ההתקשרות הראשונה, באמצעות הסיסמה הראשונית;

(2) בהתאם לרמת השירות ורמת הסיכון של המערכת, ולפחות אחת לחצי שנה.

(ד) תאגיד בנקאי יבטל את הסיסמה (להלן: סיסמה חסומה) שנמסרה ללקוח במקרים הבאים:

(1) הסיסמה הראשונית, כאמור בסעיף קטן (ב), לא הופעלה תוך 30 יום מהנפקתה;

(2) לבקשת הלקוח או כאשר התאגיד הבנקאי חושד שנעשה שימוש בלתי מורשה בסיסמה;

(3) לאחר מספר מסוים (שיקבע התאגיד הבנקאי) של ניסיונות כניסה כושלים, אשר בכל מקרה לא יעלה על חמישה ניסיונות כושלים רצופים;

(4) לאחר תקופה של חצי שנה של אי-שימוש במערכת הספציפית לה שויכה הסיסמה.

(ה) על אף האמור בסעיף קטן (ב)(2) רשאי תאגיד בנקאי לשחרר סיסמה חסומה באמצעים אחרים, ובלבד שיזוהה הלקוח, בנוסף לפרטי הזיהוי המקובלים, גם על פי פרטי זיהוי ספציפיים שנמסרו על ידו מראש לענין זה, בעת חתימת ההסכם עם הבנק או על פי פרטים (שלא עודכנו בתקשורת) שרשומים אצל התאגיד הבנקאי. בכל מקרה יתקיים האמור בסעיף קטן (ב)(1) לעיל.

הסדר זה לא יחול על סיסמה ראשונית שלא הופעלה כאמור בסעיף קטן (ד)(1).

(ו) האמור בסעיפים קטנים (ג), (ד)(1), (ד)(4) ו-(ה) לא יחול על שירותי בנקאות בתקשורת המשתמשים באמצעי זיהוי כאמור בסעיף 22(ב).

אמצעי בקרה

24. (א) בכל כניסה של הלקוח לחשבונו באמצעות שירותי בנקאות בתקשורת יוצגו בפניו, ככל שניתן, פרטים על מועד התקשרותו הקודמת באותו ערוץ.

- (ב) תאגיד בנקאי יקיים תהליך של אישור הלקוח לבצע פעולה בחשבון, שיתייחס למרכיבים העיקריים של הפעולה (סוג, מהות, סכום וכדו'). יש לאפשר ללקוח, ככל שהדבר ניתן, ביצוע שמירה/ הדפסה בזמן אמת של פרטי ההוראה שניתנה בפועל.
- (ג) תאגיד בנקאי ינקוט באמצעים שבשליטתו להגנה על מחשב/ מכשיר אחר המשמשים את הלקוח להתקשרות מפני שימוש לא מורשה וחשיפת מידע על חשבונות הלקוח (כגון: מניעת שמירת הסיסמה בדפדפן, מניעת שמירת דפי אינטרנט בזיכרון "מטמון" (Cache) וכדומה).

עסקאות בתקשורת לטובת צד שלישי

25. (א) עסקאות בתקשורת לטובת צד שלישי יבוצעו באחד מהאופנים הבאים:
- (1) עסקאות לזכות חשבונות המוגדרים ברשימת מוטבים כאמור בסעיף 26 להלן (רמת שירות (3)), בתקרות שייקבעו על ידי התאגיד הבנקאי ו/או הלקוח;
 - (2) עסקאות לזכות חשבונות אחרים (רמת שירות (4)) עד לתקרות המפורטות בסעיף קטן (ג) להלן.
- (ב) (1) הלקוח יתבקש לציין בעת מתן ההוראה, את פרטי המקבל ואת מהות התשלום.
- (2) תאגיד בנקאי יעביר נתונים על פרטי המשלם, וככל שניתן על מהות התשלום, כך שניתן יהיה להציגם באופן ברור בתמצית החשבון של המוטב.
- (ג) תקרות לעסקאות לזכות חשבונות אחרים (רמת שירות (4)):
- תאגיד בנקאי יקבע תקרה לתשלום הבודד ולסך התשלומים המתבצע מן החשבון במהלך תקופה של חודש בהתאם לסוג הלקוח, ובלבד שלא יחרוג מהתקרות כדלהלן:
- (1) במגזר העסקי תקרת תשלום בודד לא תעלה על 200,000 ש"ח, וסך התשלומים המתבצעים מן החשבון במהלך תקופה של חודש לא יעלה על 1,000,000 ש"ח;
 - (2) במגזר הפרטי תקרת תשלום בודד לא תעלה על 6,000 ש"ח, וסך התשלומים המתבצעים מן החשבון במהלך תקופה של חודש לא יעלה על 50,000 ש"ח.
- (ד) על אף האמור בסעיף קטן (א) לעיל, רשאי תאגיד בנקאי לבצע עסקאות לזכות מוטבים אחרים (רמת שירות (4)) באמצעות טכנולוגיה כאמור בסעיף 12(ג)1 ברמת העסקה הבודדת, בתקרות שייקבעו על ידי התאגיד הבנקאי ו/או הלקוח.

רשימת מוטבים

26. (א) תאגיד בנקאי ינהל רשימת מוטבים ממוכנת לכל לקוח המעוניין בשירות. רשימת המוטבים תאושר בכתב ומראש על-ידי הלקוח בסניף.
- (ב) הלקוח יהיה רשאי להעביר לתאגיד הבנקאי עדכונים לרשימת המוטבים בסניף או בתקשורת, ובלבד שתוקפו של עדכון בתקשורת יותנה בשימוש בטכנולוגיה כאמור בסעיף 12(ג)1.
- (ג) (1) לפחות אחת לשנה יידרש לקוח לאשר את רשימת המוטבים על כל פרטיה, לרבות התקרה לתשלום של כל מוטב הכלול ברשימה, אם ישנה. בדרישה לאישור רשימת המוטבים יציין התאגיד הבנקאי את ההשלכות של אי אישור הרשימה במועד, כמצויין בסעיף קטן (ד) להלן.

- (2) האישור ניתן לביצוע בכתב בסניף או על ידי משלוח מכתב למענו של הלקוח שיאושר (או יתוקן) על ידי הלקוח בחתימתו ויוחזר בדואר, או באמצעות תקשורת תוך שימוש בטכנולוגיה כאמור בסעיף 12(ג)(1).
- (3) על אף האמור בסעיף קטן (2), רשאי הלקוח לאשר את רשימת המוטבים כאמור בסעיף קטן (1), מבלי לשנותה, באמצעות מערכת בנקאות בתקשורת, ובלבד שהסכם ההתקשרות שנחתם בינו לבין התאגיד הבנקאי באותו ערוץ תקשורת, הינו לרמת שירות הגבוהה מרמת שירות (1). אישר הלקוח את רשימת המוטבים כאמור, תשלח ללקוח הודעה באמצעות הדואר אודות אישורו בתוספת רשימת המוטבים.
- (ד) רשימה שלא תאושר על ידי הלקוח בתוך 45 יום מבקשת התאגיד הבנקאי - יפוג תוקפה. על התאגיד הבנקאי ליידע את הלקוח על דרישה זו, בעת חתימתו על רשימת המוטבים כאמור בסעיף קטן (א) לעיל.

דואר אלקטרוני

27. (א) הנהלת תאגיד בנקאי תקבע את השימושים ואת סוגי הפעילויות שמותר ללקוחות התאגיד הבנקאי לבצע באמצעות דואר אלקטרוני.
- (ב) תאגיד בנקאי יביא בחשבון את מידת הצורך בזיהוי חד משמעי של לקוח השולח דואר אלקטרוני, באימות ואבטחה של תוכן המסר, בשמירה על סודיות המידע ובמניעת הכחשה, ובהתאמה לסוגי הפעילויות כאמור בסעיף קטן (א).
- (ג) על אף האמור בסעיפים קטנים (א) ו-(ב) לעיל, מתן הוראות לביצוע פעולות של לקוחות התאגיד הבנקאי (להלן: הוראות ביצוע) באמצעות דואר אלקטרוני יינתנו תוך שימוש בטכנולוגיה כאמור בסעיף 12(ג)(1).
- (ד) תאגיד בנקאי רשאי לשלוח באמצעות דואר אלקטרוני או באמצעות אתר התאגיד (להלן: אמצעים אלה), הודעות שחובת הסודיות חלה עליהן, ובלבד שיתקיימו התנאים הבאים:
- (1) (א) הלקוח חתם על הסכם כאמור בסעיף 20;
 - (ב) הלקוח יוכל להפסיק שירות זה בכל עת, לפי בקשתו;
 - (ג) העברת המידע מהבנק אל הלקוח תהיה בסביבה מאובטחת, תוך נקיטת אמצעים נאותים לשמירה על סודיות המידע;
 - (ד) במשלוח הודעות באמצעות דואר אלקטרוני, יפעיל התאגיד הבנקאי כלים ממוחשבים המאפשרים לו לקבוע חד-משמעית האם הלקוח קיבל את הדואר ופתח אותו, או ביצע הורדה (Download) של מסר הדואר למחשבו האישי או הדפסתו;
 - (ה) במשלוח הודעות באמצעים אלה ישמור התאגיד הבנקאי את המידע התפעולי הנחוץ לבדיקה ולניהול מעקב אחר קיום כללי גילוי נאות.

- (2) בהתייחס להודעות המנויות בהוראת ניהול בנקאי תקין מס' 420, ניתן להסתפק בהעברת המידע באמצעים אלה בלבד, אם התקיימו התנאים האמורים בסעיף 1 לעיל, ואם הלקוח ביקש שלא לקבל את ההודעות באמצעות דואר רגיל. לעניין זה "בקשה" - באמצעות מסמך בכתב, באמצעות אתר האינטרנט של התאגיד הבנקאי או באמצעות שיחה מוקלטת.

ריכוז מידע

28. (א) תאגיד בנקאי רשאי להציע ללקוחותיו וללקוחות תאגידי בנקאיים אחרים שירות של "ריכוז מידע" (Account Aggregation) (להלן: השירות) במודל "User Driven" (כגון תוכנה במחשב הלקוח) או במודל "הצד השלישי" (כגון באמצעות שרת של התאגיד הבנקאי).
- (ב) תאגיד בנקאי שמציע את השירות במודל "הצד השלישי" יעשה זאת באמצעות שרת ייעודי של התאגיד שנועד לשירות זה בלבד.
- (ג) מתן השירות על ידי תאגיד בנקאי יעשה בתנאים הבאים:
- (1) השירות מוגבל לריכוז מידע בלבד;
 - (2) לתאגיד הבנקאי ולעובדיו לא תהיה גישה למידע הלקוחות המתקבל מתאגידי בנקאיים אחרים (להלן: מידע הלקוחות), והם לא יעשו בו שימוש. לשם כך יישם התאגיד הבנקאי פתרונות טכנולוגיים שיתמכו בחסיון ובהגנה על המידע שמעבירים תאגידי בנקאיים אחרים על לקוחותיהם, ויספק נתיב ביקורת לנסיונות גישה למידע, לרבות המידע על אמצעי הגישה לחשבונות התאגידי האחרים;
 - (3) על אף האמור בפיסקאות (1) ו-(2), רשאי תאגיד בנקאי לעשות שימוש עצמי בלבד במידע הלקוחות המצרפי (הסה"כ) בתנאי שקיבל מהלקוח אישור מפורש לעשות זאת ושהמידע יועבר לידיעת הלקוח בלבד;
 - (4) תאגיד בנקאי יפעיל את השירות רק ביוזמת הלקוח, ובסמוך לנקודות הזמן אותן ביקש;
 - (5) תאגיד בנקאי נותן השירות לא יצבור את מידע הלקוחות על פני זמן, אלא ימחק אותו בסמוך להעברתו ללקוח;
 - (6) תאגיד בנקאי נותן השירות לא יאפשר החלפת סיסמאות של תאגידי בנקאיים אחרים באמצעות מערכת ריכוז מידע;
 - (7) (א) תאגיד בנקאי ימחק מהמאגרים הרלוונטיים את כל המידע האישי והמידע המאפשר גישה לחשבונות של לקוח המבקש להתנתק מהשירות;
(ב) המשך שמירת פרטים אישיים של משתמשים שאינם לקוחות הבנק והתנתקו מהשירות מותנה בקבלת אישור ספציפי לכך בעת ההצטרפות לשירות;
 - (8) תאגיד בנקאי לא יתנה מתן השירות בהסכמת הלקוח לאמור בפסקאות (3) ו-(7)(ב) לעיל.
- (ד) תאגיד בנקאי שיבקש לספק שירותי ריכוז מידע יפנה לקבלת היתר לכך מהמפקח על הבנקים, כמפורט בסעיף 30(א).

פרק ח': שונות**בנק חוץ**

29. ההוראה תחול כלשונה על בנק חוץ, למעט השינויים המפורטים להלן:
- (א) בכל מקום בהוראה, הביטוי "מערך טכנולוגיית מידע" יוחלף בביטוי "מערך טכנולוגיית המידע המקומי, לרבות הממשקים של מערך זה עם מערך הבנק בחו"ל".
- (ב) סעיף 3 יחול על ההנהלה במקום על הדירקטוריון.
- (ג) לסעיף קטן 11(א)(3) יתווסף המשפט:
"עותק מהתמצית הניהולית יועבר לידיעת הממונה על אבטחת המידע בבנק האם".
- (ד) לסעיף 16 להוראה יתווסף הסעיף הבא:
" (ה) בנק חוץ ישמור בכל עת, במערכות המידע המקומיות בסניפיו בישראל, נתונים מלאים המכילים את כל הפרטים האישיים והמנהליים לגבי בעלי החשבונות, מיופי הכח וזכויות החתימה, וכן את כל היתרות העדכניות של החשבונות המנוהלים בסניפיו בישראל".
- (ה) הסעיפים המפורטים להלן יכולים להתבצע על ידי בנק האם, ולא ישירות על ידי בנק החוץ, ובלבד שבנק החוץ יבצע במידת הצורך את ההתאמות הנדרשות כדי לעמוד בסעיפי ההוראה הבאים כלשונם: 5, 6(א), 6(ב), 7, 8(א), 10(א), 10(ב), 12, 13, 14, 16(ד), 21, 22, 23, 24, 25, 26, 27(ג), 27(ד)(1)(ג), 27(ד)(1)(ה), 28.
- (ו) במקרים חריגים, בנק חוץ הסבור כי סעיפים מסוימים בהוראה זו אינם ישימים לגביו, רשאי לפנות למפקח על מנת לתאם תחולתם ו/או דרך יישומם לגביו, כמפורט בסעיף 30(א).

פעולות הטעונות הסכמה ופעולות הטעונות דיווח

30. (א) תאגיד בנקאי המעוניין לבצע את אחת מהפעולות הבאות יודיע מראש למפקח. לא הודיע המפקח לתאגיד הבנקאי, תוך 90 יום, על אי אישור הפעילות, יוכל התאגיד הבנקאי לראות זאת כאישור:
- (1) שימוש בערוצי תקשורת חדשים או מכשירים חדשים לצורך בנקאות בתקשורת, שלא היו בשימוש במערכת הבנקאית בישראל;
- (א1) מינוי מנהל טכנולוגיית המידע כמפורט בסעיף 4(א1) ו/או מינוי מנהל אבטחת מידע כמפורט בסעיף 9(א1).
- (ב1) העברת מידע לתאגיד בנקאי זר בלא הצפנה כמפורט בסעיף 13(א1).
- (2) קישוריות התאגיד הבנקאי לאינטרנט על-פי סעיף 14(ב)(3);
- (3) מיקור חוץ כמפורט בסעיף 17(ב);
- (4) הצעת שירות ריכוז מידע כאמור בסעיף 28(ד);
- (5) התאמת תחולת סעיפי ההוראה עבור בנק חוץ, כמפורט בסעיף 29(ו).

תאגיד הבנקאי ידווח למפקח על הבנקים על הנושאים והאירועים הבאים:

- (1) אירועים חריגים, לרבות ניסיונות מהותיים של חדירה ותקיפה, חדירות בפועל למערכות מחשב, קריסה של מערכות מרכזיות, הפעלת תכנית החירום של התאגיד הבנקאי וכיוצא באלה;
 - (2) הפסקה של שירותים מהותיים ללקוחות כתוצאה מהשבתה לא מתוכננת של פעילות מערכות ממוכנות לפרק זמן של יותר מיום עסקים אחד;
 - (3) הקמת תאגיד עזר שעיסוקו בתחום טכנולוגיית המידע;
 - (4) החלטה על שינויים מהותיים צפויים במדיניות ניהול טכנולוגיית המידע, הסבה מהותית של מערכות המחשוב ומחשוב מחדש של מערכות מרכזיות ודומיהם;
 - (5) החלטה על הרחבת רמת השירות, שינוי מהותי בערוצי התקשורת או יוזמה חדשה במתן שירותי בנקאות בתקשורת;
 - (6) הודעה על "הסכם מקוון" (סעיף 20(ד)).
- (ג) הודעות ודיווחים לפי סעיפים (א) ו-(ב) לעיל יש לשלוח ליחידה למידע ודיווח בפקוח על הבנקים בבנק ישראל.
- (ד) דיווחים לפי סעיפים (ב) (1) ו-(ב) (2) לעיל יש לשלוח בתוך יום עסקים אחד מקרות האירוע נשוא הדיווח. הודעות לפי סעיפים (ב) (3) עד (ב) (6) יש לשלוח 30 יום מראש.

* * *

עדכונים

תאריך	פרטים	גרסה	חוזר 06 מס'
31/12/79	חוזר מקורי		830
8/91	שיבוץ בהוראות ניהול בנקאי תקין	1	----
12/95	גרסה מחודשת של קובץ ניהול בנקאי תקין	2	----
27/8/97	עדכון	3	1890
14/9/03	החלפת הוראה 357 + הוראה 412	4	2118
30/1/11	עדכון	5	2292
29/4/12	עדכון	6	2334

עדכונים הוראה 412 (בנקאות בתקשורת)

תאריך	פרטים	גרסה	חוזר 06 מס'
25/9/88	חוזר מקורי		103/16
8/91	שיבוץ בהוראות ניהול בנקאי תקין	1	----
12/95	גרסה מחודשת של קובץ ניהול בנקאי תקין	2	----
17/4/96	עדכון	3	1814
30/6/96	עדכון	4	1822
27/8/97	עדכון	5	1889
14/9/03	ביטול ההוראה		2118