

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	
בטל	שירותי בנקאות בתקשורת	פרק ז'
בטל	19. הגדרות	
בטל	20. הסכם התקשרות למתן שירותי בנקאות בתקשורת	
בטל	21. גילוי נאות	
בטל	22. אמצעי זיהוי והרשאות	
בטל	23. ניהול סיסמאות	
בטל	24. אמצעי בקרה	
בטל	25. עסקאות בתקשורת לטובת צד שלישי	
בטל	26. רשימת מוטבים	
בטל	27. דואר אלקטרוני	
בטל	28. ריכוז מידע	
357-13	שונות	פרק ח'
357-13	29. בנק חוץ	
357-13	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 תאגידי בנקאיים, וכן על תאגידיים 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) בטל;

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 נשוא הגישה.
- (2) על אף האמור בפסקה (1) לעיל, לגבי שאליות 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 שאליות 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(א3), 11(א)3, 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) (1) 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 לעניין זה.

- (1) (ג) 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.
- (ה) על אף האמור בסעיפים (א) – (ג) לעיל, על לקוחות המשתמשים בשירותי בנקאות בתקשורת כהגדרתם בהוראת נ.ב.ת. מספר 367 בנושא: "בנקאות בתקשורת" יחולו הסעיפים הרלבנטיים בהוראה זו.

הצפנה

13. תאגיד בנקאי יבחן את הצורך בהצפנה של נתונים, לרבות בתוך התקשורת, במערכות שהוגדרו בהתאם להערכת הסיכונים כבעלות סיכון גבוה, ובלבד שבמקרים הבאים תתקיים הצפנה:
- (א) בטל.
 - (א1) בטל.
 - (ב) גישה מרחוק למחשב התאגיד הבנקאי, בכפוף לאמור בסעיף 12(ג). האמור בסעיף זה אינו חל על חל לקוחות המשתמשים בשירותי בנקאות בתקשורת כהגדרתם בהוראת נ.ב.ת. מספר 367 בנושא: "בנקאות בתקשורת".
 - (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 בהוראת ניהול בנקאי תקין מספר 367;
 - (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) ושאינן 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) בטל.

(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 שנעשית מטעמו על ידי גורמים חיצוניים.

פרק ז': שירותי בנקאות בתקשורת
בטל.

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), ובכדי לעמוד בהוראת ניהול בנקאי תקין מספר 367.
- (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) בטל;
- (א1) מינוי מנהל טכנולוגיית המידע כמפורט בסעיף 4(א1) ו/או מינוי מנהל אבטחת מידע כמפורט בסעיף 9(א1).
- (ב1) בטל.
- (2) קישוריות התאגיד הבנקאי לאינטרנט על-פי סעיף 14(ב)(3);
- (3) מיקור חוץ כמפורט בסעיף 17(ב);
- (4) בטל;
- (5) התאמת תחולת סעיפי ההוראה עבור בנק חוץ, כמפורט בסעיף 29(ו).
- (ב) 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) בטל;
- (6) בטל.
- (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.
- (ה) על אף האמור בסעיפים (ב), (ג) ו- (ד) לעיל, לענין דיווח על אירוע או חשד לאירוע של תרמית בשירותי בנקאות בתקשורת וכן לגבי אירוע משמעותי הקשור לבנקאות בתקשורת לרבות ניסיונות מהותיים של חדירה וחדירות בפועל, הפסקת שירות של מערכות והונאות במערכות בנקאות בתקשורת, יחולו הוראות הדיווח המפורטות בהוראת ניהול בנקאי תקין מספר 367 בנושא "בנקאות בתקשורת".

* * *

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
21/7/16	עדכון	7	2507

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