בנק ישראל
הפיקוח על הבנקים
אגף מדיניות והסדרה

ט״ו בתמוז תשע״ו
21 ביולי 2016
חוזר ח – 06 - 2507

לכבוד
התאגידים הבנקאיים וחברות כרטיסי אשראי

הנדון: **בנקאות בתקשורת**
(ניהול בנקאי תקין הוראה מס׳ 367)

כללי

1. בשנים האחרונות חל גידול משמעותי בהיקף השימוש של לקוחות הבנקים בשירותי בנקאות בתקשורת. לצד הגידול בהיקפי השימוש, תאגידים בנקאיים חשים צורך לעדכן באופן שוטף ומהיר את השירותים והמוצרים הבנקאיים, הן בשל ציפיות הלקוחות, הן בשל ההתפתחות הטכנולוגית המהירה והן בשל תחרות הולכת וגוברת מצד חברות יזמות המציעות שירותים בנקאיים שונים.
2. פרסום הוראה ייעודית בנושא בנקאות בתקשורת בא להדגיש את החשיבות שהפיקוח על הבנקים נותן להמשך התפתחות הבנקאות הדיגיטלית, וזאת, בנוסף לסיבות שהוזכרו לעיל, גם על מנת לתמוך בתהליכי ההתייעלות הנדרשים מהם.
3. מטרת ההוראה הינה הסרת חסמים קיימים להמשך התפתחות הבנקאות הדיגיטלית ומתן גמישות בהתאם לטכנולוגיה המשתנה, וזאת מבלי שהתאגידים הבנקאיים יצטרכו לפנות לפיקוח בכל שינוי או הוספה של שירות ככל שלא מדובר בשינוי או הוספה מהותיים. אשר על כן, ההוראה בנויה בעיקרה על עקרונות וכן הנחיות ספציפיות היכן שהפיקוח סבר כי הן נדרשות. גישה מבוססת עקרונות מטילה על התאגידים הבנקאיים אחריות מוגברת ומחייבת אותם לנהוג בזהירות הנדרשת ולשפר בכל עת את המסגרת הקיימת לניהול הסיכונים ולהתאים אותה לסביבה הטכנולוגית הדינאמית בה הם פועלים.
4. בכוונת הפיקוח על הבנקים לפרסם בעתיד הוראות נוספות שישלימו את המסגרת הנדרשת לניהול הסיכונים.
5. לאחר התייעצות עם הוועדה המייעצת בעניינים הנוגעים לעסקי בנקאות ובאישור הנגידה, קבעתי את הוראת ניהול בנקאי תקין הבאה, כמפורט להלן.

מבנה ההוראה

6. ההוראה כוללת תשעה פרקים:

(א) **פרק א': כללי** - מבוא להוראה, תחולה והגדרות.

(ב) **פרק ב': ממשל תאגידי** - מפרט את תפקידי הדירקטוריון וההנהלה הבכירה.

(ג) **פרק ג': פתיחת חשבון מקוון והצטרפות לשירותי בנקאות בתקשורת** - עוסק בפתיחת חשבון מקוון, הסכם למתן שירותי בנקאות בתקשורת, הצטרפות מרחוק לשירותי בנקאות בתקשורת וכן בכריתת הסכם מרחוק.

(ד) **פרק ד': זיהוי ואימות** - מפרט את העקרונות הנדרשים בנושא זיהוי ואימות.

(ה) **פרק ה': הגנה על לקוחות** - עוסק בהדרכת לקוחות העושים שימוש בבנקאות בתקשורת ובקרות המוטמעות על ידי התאגיד הבנקאי להגנה על הלקוחות, כגון: ניטור חריגים ומשלוח התראות על פעילות חריגה, ועל פעולות בהתאם לשיקול דעתו של התאגיד הבנקאי.

(ו) **פרק ו': בקרות בבנקאות בתקשורת** - עוסק בבקרות המוטמעות בפעולות מסוימות ולרבות: עדכון פרטי חשבון, ביצוע העברות ותשלומים ואבטחת התקשורת בין הלקוח לבין התאגיד הבנקאי בערוצי הבנקאות בתקשורת.

(ז) **פרק ז': בקרות במכשירים ובערוצים ספציפיים** - עוסק בבקרות שעל התאגיד הבנקאי להטמיע בערוצים ומכשירים ספציפיים בהם נעשה שימוש בבנקאות בתקשורת, כגון: דואר אלקטרוני, מכשירים ניידים ועמדות אוטומטיות לשירות עצמי.

(ח) **פרק ח': ריכוז מידע** - מפרט את העקרונות שעל תאגיד בנקאי ליישם כאשר הוא מרכז מידע עבור לקוחות.

(ט) **פרק ט': דיווחים ואישורים** – מפרט את הדיווחים הנדרשים בנושא בנקאות בתקשורת וכן מצבים בהם יידרש לפנות לפיקוח על מנת לקבל אישור לפעילות חדשה.

פירוט לפי סעיפים

פרק א' - כללי

מבוא (סעיפים 1-6 להוראה)

7. ההוראה מסדירה את פעילות התאגידים הבנקאיים מול לקוחותיהם בתקשורת ומאפשרת פעילות מרחוק במגוון שירותים בנקאיים, כך שהלקוח יוכל לקבל שירות בכל מקום ובכל זמן.
8. ההוראה קובעת עקרונות לניהול הסיכונים בבנקאות בתקשורת, הן במערכות ובתהליכים פנימיים בתאגיד הבנקאי והן בהתנהלות מול הלקוח דרך הדרכה והגברת מודעות לסיכונים הגלומים בפעילות, ובעת התממשות סיכונים. ההוראה קובעת מגוון בקרות שעל התאגיד הבנקאי ליישם על מנת למזער את הסיכונים הנוצרים מפעילות בתקשורת, שצפויה להמשיך ולהתרחב למספר גדול יותר של לקוחות ולמגוון רחב יותר של ערוצים ושירותים.
9. המסגרת הנדרשת בהוראה לניהול סיכוני בנקאות בתקשורת הינה חלק מהמסגרת הכוללת בתאגיד הבנקאי לניהול סיכונים, המעוגנת בהוראה מס' 310 בנושא "ניהול סיכונים" ובהוראה מס' 350 בנושא "ניהול סיכונים תפעוליים" וכן בהיבטים טכנולוגיים ונוספים בהוראות שונות, וביניהן, הוראה מס' 357 בנושא "ניהול טכנולוגיית המידע" תוך תיאום להוראה 357 לרבות לעניין סעיף 3(ב) בה, וכן בהיבטים שונים להוראה 361 בנושא "ניהול הגנת הסייבר". יובהר כי אין בהפניה להוראות אלה ואחרות בבחינת החלת אותן הוראות על תאגידים בנקאיים שהוראות אלה אינן חלות עליהם.

תחולה (סעיף 7 להוראה)

10. תחולת ההוראה לבנקאות בתקשורת תואמת לתחולת הוראת ניהול בנקאי תקין מס' 357, לרבות סולק כהגדרתו בסעיף 36ט בחוק הבנקאות (רישוי), התשמ"א-1981.

הגדרות (סעיף 8 להוראה)

11. ההגדרות נועדו להבהיר את המסגרת ליישום ההוראה ולאפשר שפה אחידה והגדרת ציפיות. כך נקבעו הגדרות ל"שירותי בנקאות בתקשורת" ול"גורם אימות" בו נעשה שימוש לאורך כל ההוראה כמרכיב מרכזי במסגרת הבקרה.
12. עמדות אוטומטיות לשירות עצמי – עמדות לשירות עצמי למעט תיבת אל תור.

פרק ב' – ממשל תאגידי

דירקטוריון (סעיפים 9-12)

13. ההוראה מפרטת את תחומי האחריות של הדירקטוריון ובהם אחריות לוודא כי הסיכונים הגלומים בבנקאות בתקשורת, לרבות סיכוני אבטחת מידע, סיכוני מעילות והונאות, סיכונים משפטיים וסיכוני מוניטין מנוהלים בצורה נאותה ובהתאם למסגרת הקיימת לניהול סיכונים.
14. הדירקטוריון יסקור ויאשר את המסגרת לניהול סיכוני בנקאות בתקשורת שתעוגן במסמך מדיניות. המדיניות תכלול, בין היתר, עקרונות ופרמטרים לסיווג פעולות בבנקאות בתקשורת לפי רמות סיכון אשר ישמשו גם לקביעת אמצעי הזיהוי והאימות הנדרשים בהם. מסמך המדיניות ישולב במסמכי המדיניות הקיימים אשר מהווים חלק מהמסגרת הכללית לניהול סיכונים.

הנהלה בכירה (13-17)

15. ההנהלה הבכירה אחראית לגיבוש המדיניות והטמעתה, לקביעת תחומי אחריות ברורים ולהקצאת משאבים נאותים לניהול הסיכונים וכן לפקח על יישום המסגרת לניהול סיכוני בנקאות בתקשורת.
16. ההוראה מטילה אחריות על ההנהלה הבכירה, להגדיר תכנית לביצוע פעולות ולהגברת מודעות בקרב לקוחות לסיכונים הגלומים בבנקאות בתקשורת, מתוך ראייה כי ערנותו של הלקוח חשובה למזעור הסיכונים.

פרק ג' – פתיחת חשבון מקוון והצטרפות לשירותי בנקאות בתקשורת

פתיחת חשבון מקוון וניהולו (סעיפים 18-27)

17. ההוראה מאפשרת פתיחת חשבון ללקוח חדש או ללקוח קיים באופן מקוון בדומה לתהליך שהתאפשר בהוראה 418 "פתיחת חשבונות באמצעות האינטרנט" המבוטלת במסגרת חוזר זה.
18. הליך הזיהוי והאימות דומה לזה שנדרש בהוראה 418 (סעיפים 18 ו-21).
19. למען הסר ספק הנפקת כרטיס חיוב בתנאים הקבועים בסעיף 6א(א)(2) לצו איסור הלבנת הון (חובות זיהוי, דיווח וניהול רישומים של תאגידים בנקאיים למניעת הלבנת הון ומימון טרור), התשס"א-2001 איננה בגדר פתיחת חשבון מקוון כאמור בסעיפים 18-27 להוראה.
20. בשלב זה, לאור דרישת חתימה בחוק כרטיסי חיוב, התשמ"ו-1986, לא ניתן להשלים כריתת הסכם להנפקת כרטיס חיוב באופן מקוון.

21. בביצוע הליך "הכר את הלקוח" (סעיף 22), תתאפשר גם העברה מהתאגיד הבנקאי בו נפתח החשבון אל חשבון על שם הלקוח בתאגיד בנקאי אחר בישראל, וזאת תוך קבלת דיווח מהלקוח על הסכום המדויק שהתקבל, ולא רק העברה מהחשבון הקיים לחדש כפי שהיה עד היום.
22. נבהיר כי במעמד פתיחת חשבון בהתאם לסעיף זה התאגיד הבנקאי יהיה רשאי לצרף לקוח לשירותי בנקאות בתקשורת במסגרת הסכם פתיחת החשבון ואז יחולו הסעיפים הרלוונטיים להוראה.

הסכם למתן שירותי בנקאות בתקשורת (סעיפים 28-32)

23. יודגש כי הפיקוח על הבנקים רואה בהסכם למתן שירותי בנקאות בתקשורת כחלק מהסכם לתנאי עסק כלליים או הסכם לפתיחת חשבון עובר ושב וניהולו כאמור בסעיפים 3(א)(1) ו-3(א)(2) לכללי הבנקאות (שירות ללקוח) (גילוי נאות ומסירת מסמכים), התשנ"ב–1992, ולפיכך אין בהוראה זו כדי לגרוע מהדרישה הקבועה בכללים לפיה ההסכם יערך בכתב ויתאפשר ללקוח לעיין בו לפני הסכמתו.
24. הסכם למתן שירותי בנקאות בתקשורת יאפשר ללקוח לבחור בנפרד כל ערוץ וכל שירות כפי שיגדיר התאגיד הבנקאי. התאגיד הבנקאי רשאי להגדיר גם מקבץ שירותים או מקבץ ערוצים, לעניין זה, מקבץ ערוצים הכוונה ערוץ אחד או יותר הנחוצים לצורך תמיכה בשירות. כמו כן התאגיד הבנקאי יביא לידיעת הלקוח את הסיכונים הכרוכים בשימוש בשירותי בנקאות בתקשורת לפני שניתנת ללקוח האפשרות לאשר כי קרא את ההסכם.
יובהר כי לקוח שחתם על הסכם התקשרות למתן שירותי בנקאות בתקשורת לקבלת שירותים מסוימים בערוצים מסוימים בהתאם לסעיף 20 להוראת ניהול בנקאי תקין מס' 357, לא יידרש לחתום שוב על הסכם למתן שירותי בנקאות בתקשורת ע"פ הוראה זו עבור אותם שירותים באותם ערוצים.
יודגש כי קיימת חשיבות להצגה מעודכנת של מכלול השירותים והערוצים אליהם בחר הלקוח להצטרף, בכל עת.
25. לקוח שחתם על הסכם בנושא הוראות טלפוניות כאמור בסעיף 3(א)(9) לכללי גילוי נאות, לא יידרש לחתום על הסכם בנקאות בתקשורת לעניין קבלת הוראות לביצוע פעולות באמצעות מענה אנושי בטלפון בהתאם להוראה זו. לעניין זה יובהר כי הסכם הוראות טלפוניות יכול להיות חלק מהסכם פתיחת חשבון, הסכם תנאי עסק כלליים או הסכם הנפקה.
26. יובהר כי כלל השירותים המבוצעים באמצעות עמדות אוטומטיות לשירות עצמי מחויבים בהסכם למתן שירותי בנקאות בתקשורת. עם זאת, אם ניתנו שירותים למי שאין לו חשבון בתאגיד הבנקאי שלו שייכת עמדת השירות האוטומטית, אזי אין חובה בהסכם. כך למשל, לקוח בנק א' יוכל למשוך מזומן מעמדה אוטומטית לשירות עצמי של בנק ב', גם אם אין לו חשבון בבנק ב' ולכן הוא לא חתום מולו על הסכם למתן שירותי בנקאות בתקשורת.

הצטרפות מרחוק לשירותי בנקאות בתקשורת (סעיפים 33-38 להוראה)

27. ההוראה מאפשרת לתאגיד בנקאי לצרף מרחוק לשירותי בנקאות בתקשורת, לכל סוגי השירותים והערוצים, ללקוחות שכבר פתחו חשבון.
28. ההוראה מתייחסת לתהליכי הזיהוי הנדרשים במקרים שונים וכן לבקרות לאימות מבצע הפעולה.
29. לקוח המבקש להצטרף מרחוק, לראשונה, לשירותי בנקאות בתקשורת, ואין ברשותו עדיין אמצעי אימות מספקים על מנת לוודא את זהותו מרחוק, נדרש להליך אימות, הדומה לזה שנדרש בעת פתיחת חשבון באופן מקוון (סעיפים 35 ו-36).
30. בהצטרפות לשירותי בנקאות בתקשורת לצורך קבלת מידע בלבד או בהוספת ערוץ לצורך קבלת מידע בלבד נדרש אימות על בסיס לפחות גורם אחד, וכאשר אין ללקוח גורם אימות, נדרש שימוש בפרטי זיהוי הרשומים בחשבון וכן צירוף מספר שאלות המאפשרות אימות (כגון: פעילות בחשבון, הוראות קבע, העברת משכורת, מועדי חיובים וכיו"ב).
31. בהצטרפות לערוץ לביצוע פעולות או בהצטרפות לשירות הכולל ביצוע פעולות, בין אם באמצעות הערוץ אליו הלקוח מבקש להצטרף ובין אם בהצטרפות באמצעות ערוץ אחר אליו הלקוח מנוי, יידרש זיהוי באמצעות לפחות שני גורמי אימות מתוך גורמי האימות המופיעים בהגדרה.
32. ההוראה מוסיפה לעניין סיום התקשרות בשירותי בנקאות בתקשורת וקובעת כי הזיהוי והאימות ייעשו באותה רמת זיהוי ואימות שקבע התאגיד הבנקאי לצורך השימוש בשירות באופן שוטף.

כריתת הסכם מרחוק (סעיף 39 להוראה)

33. הסעיף מפרט הנחיות לכריתה מרחוק של הסכמים שאין חובה ע"פ דין להחתים עליהם בכתב את הלקוח. בין היתר, נקבע כי על התאגיד הבנקאי להפעיל אמצעי אשר יבטיח כי הלקוח אישר שניתנה לו אפשרות לקרוא את ההסכם וכי הסכים לתנאיו.
34. על התאגיד הבנקאי לאפשר ללקוח לעיין בהסכם בכל עת בצורה בהירה וקריאה ולהדפיסו.

<u>פרק ד' – זיהוי ואימות</u>

זיהוי ואימות (סעיפים 40-44)

35. הפרק עוסק בזיהוי ואימות של לקוחות בפעילותם בבנקאות בתקשורת.
36. תאגיד בנקאי יקבע אמצעי זיהוי ואימות אישיים בהתאם להערכת סיכונים ולמדיניות שאושרה על ידי הדירקטוריון.

37. תאגיד בנקאי ימסד תהליכים לטיפול באמצעי הזיהוי והאימות החל משלב היצירה וההעברה וכלה בשלב ההפעלה וההחלפה. במסירת אמצעי הזיהוי ללקוח, התאגיד הבנקאי נדרש לוודא כי מידע רגיש לא נחשף.

38. ניהול אמצעי הזיהוי והאימות ובכלל זה הסיסמאות, יהיה באחריות התאגיד הבנקאי ובכפוף לניהול סיכונים נאות. ההוראה לא כוללת הנחיות ספציפיות לעניין החלפת סיסמאות, שחרור שלהן או אופן העברתן ומשאירה לתאגידים הבנקאיים שיקול דעת מלא. עם זאת, יובהר כי, לא ניתן להסתפק בגורם אימות אחד בלבד (כדוגמת OTP) לצורך יצירה מחדש של גורם אימות אחר (כדוגמת סיסמה קבועה) ובכך ליצור 2 גורמי אימות באמצעות גורם אימות אחד.

39. סעיף 42 מפרט רשימה של פעולות ברמת סיכון גבוהה לגביהן יידרש שימוש בשני גורמי אימות לפחות (2FA). רשימה זו אינה ממצה והאחריות לקביעת הפעולות ברמת סיכון גבוהה הינה של התאגיד הבנקאי כאמור לעיל.

40. בחשבון הרשומים בו מספר שותפים ונדרשת בו הסכמת כל השותפים לביצוע פעולה (בהתאם להוראות רגולטוריות, הסכם או חשבון "גם וגם") תידרש הסכמת כל השותפים גם בביצוע פעולות בבנקאות בתקשורת (סעיף 43). בחשבון של תאגיד יתאפשר לגורם אחד לפעול לבד, גם אם נדרשת הסכמת השותפים, וזאת לאחר קבלת אישור מאומת מגורם מוסמך לכך בתאגיד (סעיף 44).

<u>פרק ה' – הגנה על לקוחות</u>

ניטור חריגים ופעולות ברמת סיכון גבוהה (סעיפים 45-47)

41. הגידול בפעילות בבנקאות בתקשורת מעלה חשש לגידול בסיכוני מעילות והונאות. לאור זאת, נדרשים תאגידים בנקאיים להרחיב ולשכלל את מנגנון ניטור האנומליות בחשבונות של לקוחות וכן בפעולות שאינן חריגות אך הוגדרו ברמת סיכון גבוהה, לרבות, אך לא רק, הפעולות שסווגו כך בסעיף 42 להוראה.

42. בנוסף, מנגנון הניטור יעודכן בהתאם לשיטות הונאה ואיומים לבנקאות בתקשורת שנחשפו בישראל ובעולם.

התראות ללקוחות (סעיפים 48-51)

43. תאגיד בנקאי יעשה שימוש בניטור האנומליות על מנת להתריע בפני הלקוחות במידת הצורך ולנקוט בצעדים מידיים כגון: השעיית עסקה או קבלת אישור מהלקוח לעסקה בטרם השלמתה. כמו כן, ישקול התאגיד הבנקאי בהתאם להערכת סיכונים, משלוח התראות על פעולות שונות בחשבון הלקוח כגון: העברות מעל תקרה שתיקבע, שינוי סיסמה, שינוי פרטי התקשרות.

44. התאגיד הבנקאי ישתמש בערוצי התקשרות על מנת להתריע מהר ככל האפשר תוך התחשבות ברמת הרגישות או הסיכון של הפעולה. סביר כי יעשה שימוש רב במסרונים (SMS) בשל השימוש הרחב בטלפונים ניידים והמהירות בה ההתראה עוברת, אך התאגיד הבנקאי יעשה שימוש בערוצים אחרים כאשר שליחת מסרון אינה אפשרית או בהתאם לבקשת הלקוח.
45. בחשבון בו יש שותפים תישלח ההתראה גם לשותפים האחרים על מנת שישמשו כבקרה נוספת בחשבון.

הדרכת לקוחות (סעיפים 52-55)

46. לאור הסיכונים הגלומים בפעילות בבנקאות בתקשורת, התאגידים הבנקאיים נדרשים לנקוט בצעדים על מנת להבהיר ללקוחות את מהותם (בנוסף לדרישה להציג את הסיכונים לפני אישור ההסכם), וכן, להדריך לקוחות כיצד להתגונן מפני הסיכונים ולהנחות אותם לנקוט בצעדים למזעורם הן בהיבט ההתנהגותי והן בהיבט הטכנולוגי (ולרבות התקנת תוכנות או רכיבים במכשירים ניידים). ההדרכה יכולה להינתן במגוון ערוצים דיגיטליים וכן בסניפים.
47. התאגיד הבנקאי נדרש לנהל את הסיכון הכרוך בחשד לאתר או אפליקציה מתחזה וכל הונאה או תרמית אחרת שעלולה לגרום ללקוחות לחשוף במתכוון או בשגגה מידע סודי ולרבות אמצעי זיהוי ואימות. במקרים חריגים בהם מתעורר חשד כאמור, למשל, כאשר מתעורר חשד לתרמית שעלולה להשפיע על מספר רב של לקוחות ובפרק זמן קצר, התאגיד ימסור הודעה על כך ללקוחותיו שנמצאים בסיכון.

<u>פרק ו' – בקרות בבנקאות בתקשורת</u>

עדכון פרטי חשבון (סעיפים 57-59)

48. עדכון פרטי התקשרות או עדכון שם בעל החשבון הינם פעולות שהוגדרו ברמת סיכון גבוהה ולכן רמת האימות שנדרשת בהן הינה לפחות 2FA. כמו כן, יבצע תאגיד בנקאי מעקב מוגבר (כגון: ספים מחמירים לניטור) אחר חשבונות בהם בוצעה פעילות חריגה שנוגעת לעדכון מרחוק של פרטי חשבון (כגון: עדכון בו-זמנית של מספר פרטים) וזאת, למשך תקופה שתיקבע על ידי התאגיד הבנקאי ובהתאם להערכת סיכונים.

העברות, תשלומים ופעולות אחרות (סעיפים 60-62)

49. בהעברות ותשלומים למוטבים, התאגידים הבנקאיים יקבעו שני ספים לביצוע פעולות: סף ראשון שמעליו יידרש שימוש ב-2FA וסף שני שמעליו יידרש שימוש בטכנולוגיה המשלבת זיהוי ואימות, סודיות ושלמות הנתונים ומניעת הכחשה. נדגיש כי הגדרת מוטב בהוראה זו אינה כוללת מוטב המוקם בהתאם להוראת ניהול בנקאי תקין מספר 439.

50. הספים יכולים להיקבע פרטנית או לפי קבוצות של לקוחות או סוגי מוטבים תוך התחשבות בשיקולי אבטחת מידע.

אבטחת ערוצי התקשורת (סעיפים 63-65)

51. כאשר תאגיד בנקאי מקבל מידע מלקוחות, אשר חלה עליו חובת סודיות, או מוסר מידע כאמור ללקוחותיו, הוא נדרש להשתמש באלגוריתם הצפנה על מנת להגן על המידע העובר ברשתות חיצוניות ולרבות האינטרנט.
52. הצפנה לא תידרש במסירת התראות ללקוחות כנדרש בהוראה וכן בהעברת מידע בדואר אלקטרוני בנוגע לחשבון של בנק זר בהתקיים התנאים המפורטים בהוראה.

<u>פרק ז' - בקרות במכשירים ובערוצים ספציפיים</u>

פעילות לקוחות באמצעות דואר אלקטרוני (סעיף 66)

53. על אף האמור בסעיף "אבטחת ערוצי התקשורת", בקבלת מידע מלקוח בדואר אלקטרוני ישקול התאגיד הבנקאי את הצורך בהצפנה והטמעת בקרות נוספות הנוגעות לאבטחת מידע, בהתאם להערכת סיכונים.

משלוח מסרונים (סעיף 67)

54. מאחר ולא ניתן לעשות שימוש באלגוריתם הצפנה בעת משלוח מסרונים, אין לכלול פרטים מזהים מלאים על הלקוח ועל חשבונו בעת העברת מידע באמצעות תווך זה.

שימוש במכשירים ניידים (סעיפים 68-70)

55. עליה בשימוש במכשירים הניידים לצורך התקשרות מרחוק, ובמיוחד במכשירי טלפון ניידים, מחייבת את הבנקים להעריך את הסיכונים הספציפיים הגלומים בהם, ולבחון הטמעת תהליכים ובקרות למזעור הסיכונים. כך למשל, תאגיד בנקאי יביא בחשבון היבטים של אבטחה פיזית של המכשירים, לרבות נעילה או התקנה של תוכנות הגנה, וכן טיפול בגניבה או אובדן לרבות ביטול השימוש בו לפעולות מסוימות ובמיוחד לשליחת התראות ו-OTP. התאגיד הבנקאי יפרסם מספר טלפון לדיווח על מכשיר שנגנב או אבד.
56. בין התהליכים שניתן ליישם, תאגיד בנקאי ישקול רישום של המכשירים הניידים בהם נעשה שימוש ורישום פרטים מזהים של המכשיר שיאפשרו זיהוי שלו בעת ביצוע פעולה.

עמדות אוטומטיות לשירות עצמי (סעיף 71)

57. תאגיד בנקאי יישם בקרות בעמדות אוטומטיות לשירות עצמי, למניעת מעילות והונאות וביניהן תמיכה בכרטיס חכם (כמשמעו בהוראת ניהול בנקאי תקין מס' 470 בנושא "כרטיסי חיוב"), והטמעת נתיב בקרה.

58. הוראות לביצוע פעולות בטלפון ע"י מענה אנושי (סעיף 72) סעיף זה מקורו בהוראת ניהול בנקאי תקין מס' 435 בנושא "הוראת טלפוניות" והוא שובץ בהוראה לנוכח ביטולה של הוראת ניהול בנקאי תקין מס' 435.

<u>פרק ח' – ריכוז מידע</u>

שירותי ריכוז מידע (סעיף 73)

59. נקבעו כללים למתן שירותי ריכוז מידע (Account Aggregation). התנאים שמעמידה ההוראה לתאגיד בנקאי המבקש להציע שירותים של ריכוז מידע נועדו, בין היתר, לשמור על חסיון המידע של הלקוח, ולהסדיר שימוש במידע של הלקוח מתאגידים בנקאיים אחרים.

60. בין היתר נקבע, כי תאגיד בנקאי יישם אמצעים להגנה מפני שימוש במידע זה. הכוונה היא להבטיח שתאגיד בנקאי, בין באמצעות טכנולוגיה ובין באמצעות עובדיו, לא ייגש ולא יעשה שימוש במידע של הלקוח שמתקבל מתאגידים בנקאיים אחרים, זולת אם קיבל מהלקוח אישור מפורש לעשות כן, וזאת, על מנת להציע ערך ללקוח בנוגע לכלל חשבונותיו ושהמידע יועבר לידיעת הלקוח בלבד.

61. יצוין כי המגבלה הכתובה בסעיף 17 (ג) להוראת ניהול בנקאי תקין מס' 357 נמחקה, ומעתה יתאפשר מיקור חוץ של שירותי ריכוז מידע, בכפוף לאישור הפיקוח על הבנקים.

<u>פרק ט' – דיווחים ואישורים</u>

דיווחים ואישורים (סעיפים 74-76)

62. נקבעו פעולות לגביהן נדרש להודיע למפקח או לקבל הסכמתו.

63. נושאים הדורשים דיווח כוללים אירועים חריגים הקשורים בפעילות בבנקאות בתקשורת שיש בהם חשש להתממשות סיכון העלול להשפיע על מספר רב של לקוחות בפרק זמן קצר, כגון: גילוי של אתר מתחזה או תרמית אחרת וכן ניסיונות חדירה מהותיים וחדירות בפועל שעלולים לגרום להפסקת פעילות.

64. נושאים הדורשים הסכמת הפיקוח, כוללים פעילות טכנולוגית חדשה מהותית המובאת לאישור הדירקטוריון. בנושאים נוספים, הפיקוח מצפה כי כאשר יש ספק בדבר הצורך לפנות לפיקוח, התאגיד הבנקאי ייוועץ עמו בפרק זמן סביר מראש לפני התחלת הפעילות החדשה.

בכל מקרה תידרש הסכמת הפיקוח להציע שירותי ריכוז מידע. הפנייה לפיקוח תיעשה לפחות 60 יום לפני תחילת הפעילות.

נושאים נוספים

ביטול הוראות ואישורים קיימים

65. החל ממועד תחילת הוראה זו יבוטלו ההוראות והאישורים הבאים:

(א) הוראת ניהול בנקאי תקין מס' 357 "ניהול טכנולוגיית המידע" סעיפים 3(ב)(5), 13(א), 13(א1), 17(ג), 19 עד 28, 30(א)(1), (21ב) ו- (4), ו- 30(ב) (5) ו- (6).

(ב) האישורים שניתנו על ידי המפקח או מי מטעמו בהתאם לסעיף 30 להוראה 357 ונוגעים לסעיפים שבוטלו לעיל, ולמעט אישורים שניתנו לשירותי ריכוז מידע. ככל שתאגיד בנקאי אוחז באישור המתיר פעילות שאינה עומדת בהנחיות הוראה זו, יודיע התאגיד למפקח על הבנקים על מנת לברר את עניינו.

(ג) הוראת ניהול בנקאי תקין מס' 418 "פתיחת חשבונות באמצעות האינטרנט".

(ד) הוראת ניהול בנקאי תקין מס' 435 "הוראות טלפוניות".

כמו כן, החל ממועד תחילת הוראה זו יעודכנו הסעיפים הבאים בהוראת ניהול בנקאי תקין מס' 357:

(ה) לסעיף 12 יתווסף סעיף קטן (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".

(ו) לסעיף 14(ב)(2) יתווספו המילים: "כמפורט בהוראת ניהול בנקאי תקין מספר 367".

(ז) בסעיף 29 (ה) יימחקו ההפניות הבאות: "21, 22, 23, 24, 25, 26, 27(ג), 27(ד)(1)(ג), 27(ד)(1)(ד), 27(ד)(1)(ה), 28" ובמקומן יתווספו המילים הבאות: "ובכדי לעמוד בהוראת ניהול בנקאי תקין מספר 367".

(ח) לסעיף 30 יתווסף סעיף קטן (ה): "על אף האמור בסעיפים (ב), (ג) ו – (ד) לעיל, לעניין 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".

תחילה

66. תחילת האמור בהוראה זו היא מיום 1.1.2017, למעט סעיף 71 (ב) (תמיכה פונקציונאלית לביצוע עסקאות בכרטיס חכם בעמדות אוטומטיות לשירות עצמי המשמשות למשיכת מזומן) שיכנס לתוקף ביום ה- 1.1.2018.
67. תאגיד בנקאי רשאי לפעול ע"פ הוראה זו במועד מוקדם יותר מהמועד הקבוע בסעיף 66 לעיל, ובלבד שיחול עליו גם סעיף 65 לעיל מאותו מועד.
68. בחר תאגיד לעשות כאמור בסעיף 67 לעיל, יודיע למפקח על הבנקים 30 יום קודם למועד כאמור.

עדכון הקובץ

69. מצ"ב דפי עדכון לקובץ ניהול בנקאי תקין. להלן הוראות העדכון:

להוציא עמוד	**להכניס עמוד**
357-1-20 [6] (4/12)	357-1-14 [7] (7/16)
-----	367-1-14 [1] (7/16)
418-1-3 [2] (2/16)	-----
435-1 [3] (1/15)	-----

בכבוד רב,

ד"ר חדוה בר

המפקחת על הבנקים

ניהול טכנולוגיית המידע

תוכן העניינים

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)(3א), 11(א)(3ב) 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)(3א), 11(א)(3ב), 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 ושאילתות 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 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.

(1א) 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)(3א), 11(א)(3ב), 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 בפיסקה (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 ובנסיונות 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.

(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 בפיסקה (1) לעיל, רשאי תאגיד בנקאי להשתמש בטכנולוגיה חלופית במקרים הבאים:

- במערכות בסיכון גבוה שלא באמצעות גישה מרחוק, על פי שיקול דעתו של התאגיד הבנקאי, שתתועד 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 בתווך 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) ושאין 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': <u>שירותי בנקאות בתקשורת</u>

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;

(1א) מינוי מנהל טכנולוגיית המידע כמפורט בסעיף 4(א1) ו/או מינוי מנהל אבטחת מידע כמפורט בסעיף 9(א)(1א).

(1ב) 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 בפיקוח 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, לעניין 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".

* * *

<u>עדכונים</u>

חוזר 06 מס'	גרסה	פרטים	תאריך
830		חוזר מקורי	31/12/79
-----	1	שיבוץ בהוראות ניהול בנקאי תקין	8/91
-----	2	גרסה מחודשת של קובץ ניהול בנקאי תקין	12/95
1890	3	עדכון	27/8/97
2118	4	החלפת הוראה 357 + הוראה 412	14/9/03
2292	5	עדכון	30/1/11
2334	6	עדכון	29/4/12
2507	7	עדכון	21/7/16

<u>עדכונים הוראה 412 (בנקאות בתקשורת)</u>

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

בנקאות בתקשורת

תוכן העניינים

פרק א': כללי

מבוא

1. בשנים האחרונות, לקוחות התאגידים הבנקאיים עושים שימוש הולך וגובר בטכנולוגיה ובערוצים ישירים על מנת לצרוך שירותי בנקאות. תופעה זו ניכרת גם בעולם. הרחבת שירותי הבנקאות בתקשורת וסוגי השירותים ובכללם בנקאות באמצעות האינטרנט, הטלפון ובאמצעות עמדות אוטומטיות לשירות עצמי, מאפשרת להוזיל את מחירי השירותים ללקוחות, וכן מקלה עליהם לנהל את פעילותם באופן עצמאי ונוח מכל מקום, בכל זמן, בערוצים שונים וללא תלות בשעות הפעילות של סניפי התאגיד הבנקאי. בנוסף, פיתוח והרחבת שירותי בנקאות בתקשורת צפויים לאפשר לתאגידים הבנקאיים להתייעל לאורך זמן.

2. במקביל ליתרונות הבנקאות בתקשורת כאמור, הגידול בהיקף השירותים הבנקאיים באמצעים טכנולוגיים ומתן אפשרות ללקוחות לבצע פעילות בנקאית מרחוק, טומנים בחובם גידול בסיכונים הייחודיים הגלומים בפעילות זו וביניהם: סיכוני אבטחת מידע וסייבר, סיכוני פגיעה בפרטיות, סיכוני מעילות והונאות, סיכוני ציות, סיכוני הלבנת הון, סיכונים משפטיים וסיכוני מוניטין.

3. על מנת להתמודד עם סיכונים אלו, התאגידים הבנקאיים נדרשים לחזק ולהתאים את המסגרת לניהול הסיכונים לסביבת הפעילות הטכנולוגית המתקדמת ולעדכן אותה באופן שוטף ודינאמי בשל המהירות בה הטכנולוגיה משתנה. זאת, תוך הקפדה, כל העת, על עקרונות אבטחת המידע הכוללים, בין היתר: שמירה על סודיות המידע של הלקוח והגנה על הפרטיות, שלמות המידע וזמינות שירותי הבנקאות בתקשורת. יובהר כי תאגיד בנקאי אשר חלות עליו הוראות ניהול בנקאי תקין: הוראה מספר 310 בנושא "ניהול סיכונים", הוראה מספר 350 בנושא "ניהול סיכונים תפעוליים", הוראה מספר 357 בנושא "ניהול טכנולוגיית המידע" והוראה מספר 361 בנושא "ניהול הגנת הסייבר" נדרש לעשות כן בהתחשב בהוראות האמורות.

4. בנוסף, נדרשים התאגידים הבנקאיים לפתח ולשכלל את השיטות לאיתור מעילות והונאות, למניעה של הלבנת הון ולטיפול בצורה מהירה ונכונה בכשלים, על מנת למזער פגיעה בלקוח, סיכונים משפטיים וסיכוני מוניטין שכרוכים בפעילות בתקשורת ונובעים גם מתוך הגידול בכמות והיקף מאגרי המידע.

5. הוראה זו מסדירה את פעילות התאגידים הבנקאיים במתן שירותי בנקאות בתקשורת ללקוחות. ההוראה מאפשרת לתאגידים הבנקאיים להציע ללקוחותיהם שירותים בנקאיים, החל מפתיחת חשבון מרחוק ללא הגעה לסניף התאגיד הבנקאי, הצטרפות לשירותי בנקאות בתקשורת באופן מקוון גם בחשבון קיים, וכלה בפעילות שוטפת, ללא צורך בהגעה לסניף או שימוש בפקס. בכך ההוראה מאפשרת ללקוחות ולתאגידים הבנקאיים להרחיב את הפעילות הדיגיטלית וליהנות מיתרונותיה כאמור, וכמו כן, מקלה על שחקנים חדשים, להם אין רשת סניפים, להיכנס לתחום הפעילות פיננסית

ובכך להגביר את התחרות. עם זאת, הרחבת האפשרויות לפעילות בנקאית מרחוק מותנית בחיזוק ושכלול ניהול הסיכונים, והבקרות על-ידי התאגידים הבנקאיים וביניהן: בקרות לזיהוי ואימות הלקוח, ייזום והעברת התראות ללקוחות, ניטור אנומליות בפעילות מסוג זה ברמת הלקוח וברמת הבנק, ועוד.

6. על מנת לתת מענה לפעילות בנקאית מלאה ולצמצם את הצורך בהגעת הלקוח לסניף, תאגידים בנקאיים נדרשים לבחון אפשרויות להציע ללקוחותיהם שירותים משלימים והכל במסגרת המגבלות הקבועות בדין.

תחולה

7. (א) הוראה זו תחול על התאגידים הבאים כהגדרתם בחוק הבנקאות (רישוי), התשמ"א 1981 (להלן בהוראה זו - "תאגיד בנקאי"):

(1) תאגיד בנקאי;

(2) תאגיד כאמור בסעיפים 11 (א) (3א) ו-(3ב);

(3) תאגיד כאמור בסעיף 11 (ב);

(4) סולק כהגדרתו בסעיף 36ט.

(ב) המפקח רשאי לקבוע הוראות מסוימות שונות מאלו המפורטות להלן שיחולו על תאגיד בנקאי מסוים או לפטור במקרים חריגים תאגיד בנקאי מסוים מהוראה מסוימת.

הגדרות

8.

"שירותי בנקאות בתקשורת" שירותים בנקאיים הניתנים באחד או יותר מהערוצים הבאים:

(א) ערוצי האינטרנט, לרבות:

(1) אתר האינטרנט;

(2) יישומון (אפליקציה);

(3) דואר אלקטרוני;

(4) תוכנות למשלוח מסרים מידיים (Instant Messaging Services);

(ב) ערוצי טלפוניה קווית וסלולרית, למעט פקס, ולרבות:

(1) מענה אנושי;

(2) מענה קולי אינטראקטיבי (IVR - Interactive Voice Response);

(3) מסרונים (הודעות SMS);

(ג) עמדות אוטומטיות לשירות עצמי.

"גורם אימות" אחד מאלה:

(א) פריט הנמצא ברשות המשתמש (לדוגמה: סיסמה חד פעמית זמנית (**OTP-One Time Password**) הנוצרת על ידי רכיב חומרה הנמצא בידי המשתמש ומקושר לחשבון שלו, סיסמה זמנית הנוצרת על ידי התאגיד הבנקאי ומועברת ללקוח על ידי מסרון או תעודה דיגיטלית הנשמרת בכרטיס חכם או רכיב אחר אשר ברשות המשתמש);

(ב) פריט הידוע רק למשתמש (לדוגמה: סיסמה קבועה);

(ג) פריט שהוא המשתמש (לרבות מאפיין ביומטרי, כגון: זיהוי קולי, טביעת אצבע וזיהוי פנים).

"הצו" צו איסור הלבנת הון (חובות זיהוי, דיווח וניהול רישומים של תאגידים בנקאיים למניעת הלבנת הון ומימון טרור), התשס"א-2001.

"חברת כרטיסי אשראי" תאגיד עזר, כאמור בסעיף 11(ב) לחוק הבנקאות (רישוי), התשמ"א-1981.

"חשבון מקוון" חשבון כהגדרתו בצו, שנפתח בהתאם להוראה זו.

"מוטב" למעט מוטב שמוקם בהתאם להוראת ניהול בנקאי תקין מספר 439.

"מכשיר נייד" לרבות מחשב נייד, מחשב לוח, טלפון נייד.

"שירותים בנקאיים" כהגדרת "שירות" בחוק הבנקאות (שירות ללקוח), התשמ"א-1981, לרבות קבלת מידע, ריכוז מידע, ביצוע פעולות ומתן הוראות לביצוע פעולות.

פרק ב': <u>ממשל תאגידי</u>

<u>דירקטוריון</u>

הדירקטוריון אחראי:

9. לוודא כי מכלול הסיכונים הגלומים בבנקאות בתקשורת, ובכלל זה סיכוני אבטחת מידע וסייבר, סיכוני פגיעה בפרטיות, סיכוני מעילות והונאות, סיכונים משפטיים, סיכוני ציות, סיכוני הלבנת הון, סיכוני מוניטין וסיכונים אסטרטגיים, מנוהל בהתאם לעקרונות המפורטים בהוראת ניהול בנקאי תקין מספר 310 בנושא "ניהול סיכונים" ובהוראת ניהול בנקאי תקין מספר 350 בנושא "ניהול סיכונים תפעוליים" וכן בהתאם להוראות הייעודיות השונות וביניהן, הוראת ניהול בנקאי תקין מספר 357 בנושא "ניהול טכנולוגיית המידע" והוראת ניהול בנקאי תקין מספר 361 בנושא "ניהול הגנת הסייבר".

10. לסקור ולאשר מסגרת לניהול סיכוני בנקאות בתקשורת שתעוגן במסמך מדיניות.
המדיניות תכלול התייחסות, בין היתר, לנושאים הבאים:

(א) ערוצי התקשרות וכן מוצרים וסוגי שירותים מותרים בכל אחד מערוצי ההתקשרות;

(ב) עקרונות ופרמטרים לסיווג הפעולות בבנקאות בתקשורת לפי רמת סיכון, הן ברמת העסקה הבודדת והן בראייה רוחבית, שעל בסיסם ייקבעו, בין היתר, אמצעי הזיהוי וגורמי האימות שיידרשו, בכפוף לדין;

(ג) פתיחת חשבון מקוון וניהולו בהתייחס, בין היתר, לבקרות, למגבלות ולמסמכים הנוספים על הקבוע בהוראה זו, בהתאם לגישה מבוססת סיכון, על מנת להפחית את הסיכונים הכרוכים בפעילות זו, ברמת החשבון הבודד וברמת התאגיד הבנקאי.

(ד) בקרות בבנקאות בתקשורת, לרבות:

(1) זיהוי ואימות של לקוחות, בין היתר, לפי סוג הלקוח, סוג הפעולה ורמת הסיכון הגלום בה;

(2) ניטור פעילות חריגה (אנומליות), ברמת הלקוח וברמת הבנק, פעולות ברמת סיכון גבוהה ומתן התראות ללקוחות;

(3) הגברת מודעות לקוחות והדרכתם;

(4) בקרות בערוצים ספציפיים;

(5) עקרונות אבטחת מידע בתקשורת בין הלקוח לתאגיד הבנקאי.

11. לוודא כי ניהול סיכוני בנקאות בתקשורת בקווי ההגנה הראשון והשני יבחן באופן תקופתי על ידי הביקורת הפנימית על בסיס ההנחיות המפורטות בהוראה 307 "פונקציית הביקורת הפנימית", ככל שהוראה זו חלה על התאגיד.

12. לקבוע דיווחים נדרשים בנושא בנקאות בתקשורת, לרבות: כשלים מהותיים במתן שירותים והטיפול בהם.

הנהלה בכירה

ההנהלה הבכירה אחראית:

13. לגבש ולהטמיע מדיניות שתעגן את המסגרת לניהול סיכוני בנקאות בתקשורת.
14. לוודא כי נקבעו תחומי אחריות ברורים והוקצו משאבים נאותים לניהול סיכוני בנקאות בתקשורת, לרבות מנהלים ועובדים בעלי כישורים וניסיון מתאימים.
15. ליישם תהליכים לפיקוח על הטמעת המסגרת לניהול סיכונים בבנקאות בתקשורת, ולרבות: דיווחים על תוצאות הערכת סיכונים והטמעת בקרות מתאימות, תוצאות תהליכי ניטור במערכות מרכזיות וכשלים משמעותיים בזמינות מערכות בבנקאות בתקשורת.
16. להגדיר תכנית לביצוע פעולות שוטפות להגברת מודעות הלקוחות לסיכונים הגלומים בפעילות בבנקאות בתקשורת.
17. לעקוב אחר התפתחויות טכנולוגיות בתחום הבנקאות בתקשורת והסיכונים הכרוכים בהן.

פרק ג': פתיחת חשבון מקוון והצטרפות לשירותי בנקאות בתקשורת

פתיחת חשבון מקוון וניהולו

18. תאגיד בנקאי המאפשר פתיחת חשבון מקוון רשאי לאמת את פרטי זהותו של המבקש לפתוח חשבון על בסיס העתק של תעודת הזהות ולא על בסיס תעודת הזהות או העתק מאושר שלה, ובלבד שהמבקש לפתוח חשבון הציג העתק ממסמך זיהוי נוסף שהנפיקה מדינת ישראל הנושא את שם הלקוח, מספר תעודת הזהות שלו ותאריך הלידה, וזאת, על אף האמור בסעיף 3(א)(1) לצו. יובהר כי אין שינוי בשאר החובות מכוח סעיף זה.
19. המבקש לפתוח חשבון מקוון הוא יחיד תושב ישראל שמלאו לו 18 שנה. המבקש או המבקשים לפתוח חשבון יהיו הבעלים, ולא יהיו נהנים בחשבון זולת הבעלים. לאחר פתיחת החשבון לא תתאפשר הוספת או שינוי בעלים בחשבון.
20. המבקש לפתוח חשבון מקוון יחתום על הצהרת נהנים באופן מקוון. התאגיד הבנקאי יתעד את הלקוח מצהיר בקולו כי אין נהנים מלבד בעל החשבון, וישמור תיעוד זה.
21. תאגיד בנקאי יזהה פנים אל פנים ויבצע הליך "הכר את הלקוח" בפתיחת חשבון מקוון באמצעות טכנולוגיית היוועדות חזותית (Video Conference) שתאפשר זיהוי ברור, וישמור תיעוד של פעולות אלה. על אף האמור לעיל, תאגיד בנקאי יהיה רשאי לבצע את הליך "הכר את הלקוח" באופן מקוון, שאינו היוועדות חזותית, לאחר שנקט באמצעים לוודא כי המשיב הוא מי שזוהה פנים אל פנים, כאמור ברישא של סעיף זה, ושמר תיעוד של ההליך.
22. התאגיד הבנקאי יבצע הליך "הכר את הלקוח" מוגבר, בדומה להליך המבוצע ביחס ללקוח בסיכון גבוה אחר, לרבות אי-ביצוע פעולות בחשבון מקוון בטרם ביצוע העברה

בנקאית באמצעות חשבון, על שם המבקש לפתוח חשבון, בתאגיד בנקאי בישראל. במקרה שהבקשה לפתוח חשבון נעשתה מתוך אתר האינטרנט של התאגיד הבנקאי, באמצעות חשבון קיים, ולאחר אימות הלקוח באמצעות 2 גורמי אימות לפחות, לא יידרש ביצוע העברה בנקאית כאמור.

23. בחשבון לא יפעל "מורשה חתימה" כהגדרתו בסעיף 1 לצו.

24. בטופסי שיקים שתאגיד בנקאי מנפיק ללקוחו, יהיו השיקים משורטטים ויהיו מודפסות עליהם מילים האוסרות את העברתם. בנוסף על האמור, יקבע הבנק בקרות ומגבלות על כמות פנקסי השיקים המונפקים ללקוח.

25. חשבון מקוון יסומן ויזוהה ככזה במערכות המחשב של התאגיד הבנקאי לצורך ניטור סיכונים וביצוע מעקב מוגבר למשך תקופה שתיקבע ובהתאם להערכת סיכונים.

26. תאגיד בנקאי, שאינו חברת כרטיסי אשראי, ישייך את החשבון שנפתח לסניף וישלח הודעה ללקוח עם פרטי הסניף אליו שויך חשבונו.

27. (א) תאגיד בנקאי רשאי להסיר את ההגבלות על חשבון שנפתח באופן מקוון, כמפורט בפרק זה, לאחר השלמת הזיהוי המלא של הלקוח בהתאם להוראות הצו.

(ב) בנוסף לאמור בסעיף 24 להוראה 411, תאגיד בנקאי שמזהה, אגב פתיחה או ניהול של חשבון מקוון, כי מדובר בלקוח בסיכון גבוה, רשאי לא לפתוח חשבון או לחסום את הפעילות בחשבון קיים, לפי העניין, עד להשלמת הזיהוי המלא של הלקוח כאמור בהוראות הצו.

<u>הסכם למתן שירותי בנקאות בתקשורת</u>

28. תאגיד בנקאי יתקשר עם לקוח בהסכם למתן שירותי בנקאות בתקשורת (להלן: "הסכם בנקאות בתקשורת").

29. על אף האמור בסעיף 28 לעיל:

(א) תאגיד בנקאי רשאי למסור מידע ללקוח על חשבונותיו באמצעות מענה אנושי, גם אם הלקוח אינו צד להסכם בנקאות בתקשורת.

(ב) תאגיד בנקאי רשאי לשלוח סיסמה חד פעמית זמנית באמצעות מסרונים, או התראות ובקשות אישורים כאמור בסעיפים 48-51 להלן, גם אם הלקוח אינו צד להסכם בנקאות בתקשורת באותו ערוץ.

(ג) תאגיד בנקאי לא יידרש להתקשר בהסכם בנקאות בתקשורת עם מי שעושה שימוש בעמדות אוטומטיות לשירות עצמי של התאגיד לקבלת שירות מזדמן, כדוגמת תשלום שוברים או משיכת מזומנים.

30. לעניין מסירת הודעות של לקוח למנפיק, יש לפעול בהתאם לחוק כרטיסי חיוב, התשמ"ו 1986, ותקנותיו, גם אם הלקוח אינו צד להסכם בנקאות בתקשורת.

31. ההסכם יאפשר ללקוח לבחור בנפרד כל שירות ע"פ הגדרת התאגיד, וכל ערוץ שמוצע על ידי התאגיד הבנקאי. על אף האמור, במקרים בהם נחוץ מקבץ ערוצים לצורך מתן שירות מסוים, רשאי התאגיד הבנקאי להציגם יחד בהסכם. הלקוח יכול להפסיק את ההתקשרות לקבלת שירות, ערוץ או מקבץ ערוצים בכל עת.
32. לפני קבלת אישור הלקוח להסכם יציג התאגיד הבנקאי את שירותי הבנקאות בתקשורת המותרים בכל ערוץ, את הסיכונים הקשורים בשימוש בשירותים אלו, ויביא לידיעת הלקוח את עקרונות אבטחת המידע והגנת הפרטיות המומלצים ליישום בידי הלקוח, על מנת למזער סיכונים אלה.

<u>הצטרפות מרחוק לשירותי בנקאות בתקשורת</u>

33. לקוח יוכל להצטרף לערוץ או לשירות תוך שימוש בלפחות שני גורמי אימות (Two Factor Authentication להלן "2FA") .
34. בהצטרפות לשירותי בנקאות בתקשורת עבור קבלת מידע בלבד, ובחברות כרטיסי אשראי גם מתן אשראי, ובלבד שהאשראי לא יחרוג ממסגרת האשראי הלא מנוצלת של הלקוח, רשאי התאגיד הבנקאי לצרף את הלקוח תוך שימוש בגורם אימות אחד לפחות או שימוש בפרטי זיהוי ומספר שאלות אשר להערכת התאגיד הבנקאי המענה עליהן מאפשר אימות של הלקוח.
35. בנוסף לאפשרויות המפורטות בסעיפים 33 ו- 34 לעיל, רשאי תאגיד בנקאי לאפשר ללקוח אשר לו חשבון בתאגיד הבנקאי, להצטרף לשירותי בנקאות בתקשורת, באמצעות טכנולוגיית היוועדות חזותית (Video Conference) שתאפשר זיהוי פנים אל פנים באופן ברור, תוך אימות פרטי זהותו של הלקוח על בסיס העתק של תעודת הזהות לפחות, וכן מול פרטי ההזדהות המצויים ברשות התאגיד הבנקאי.
36. לעניין אימות פרטי זהותו של הלקוח כאמור בסעיף 35 לעיל, רשאי התאגיד הבנקאי לאמת את פרטי זהותו של לקוח שהוא תושב חוץ, על בסיס העתק של דרכון, וכן מול פרטי ההזדהות המצויים ברשות התאגיד הבנקאי.
37. תאגיד בנקאי המאפשר ללקוח להצטרף מרחוק לשירותי בנקאות בתקשורת כאמור בסעיפים 35 ו - 36 לעיל, יצור קשר עם הלקוח, באמצעי התקשורת הרשומים אצלו בחשבון, על מנת לוודא כי אכן ביקש להצטרף לשירותי בנקאות בתקשורת, אלא אם כן זיהוי הפנים אל פנים באמצעות טכנולוגיית היוועדות חזותית כאמור בסעיף 35 לעיל, נעשה ע"י אמצעי התקשורת הרשומים בחשבון הלקוח.
38. סיום התקשרות לקבלת שירות בערוצי בנקאות בתקשורת ייעשה באותה רמת זיהוי ואימות שמשמשת לצורך קבלת השירות בהתאם לסעיף 40 להלן.

כריתת הסכם מרחוק

39. בכריתת הסכם מרחוק יפעיל התאגיד הבנקאי אמצעי על מנת לוודא שהלקוח אישר כי ניתנה לו אפשרות לקרוא את ההסכם והסכים לתנאיו. נוסח ההסכם אותו אישר הלקוח, יהיה זמין לעיונו בכל עת בצורה בהירה וקריאה וניתן יהיה להדפיסו.

פרק ד': זיהוי ואימות

40. תאגיד בנקאי יקבע אמצעי זיהוי ואימות אישיים בפעילות בבנקאות בתקשורת בהתאם להערכת סיכונים ולמדיניות שאושרה על-ידי הדירקטוריון.

41. תאגיד בנקאי ימסד תהליכים לאופן היצירה, המסירה, ההפעלה וההחלפה של כל אמצעי הזיהוי והאימות, שיאפשרו לו לוודא, בין היתר, כי מידע רגיש לא ייחשף בתהליך היצירה והמסירה. בשימוש בסיסמאות יקבעו כללים לאופן קביעת הסיסמה מבחינת אורך והרכב, מגבלות לשימוש חוזר, תדירות החלפתה, חסימה ושחרור סיסמה.

42. פעולות, שיוגדרו ברמת סיכון גבוהה, בהתאם לעקרונות שאושרו על-ידי הדירקטוריון, יתאפשרו רק לאחר אימות באמצעות לפחות שני גורמי אימות.
פעולה ברמת סיכון גבוהה תכלול, לכל הפחות:

(א) העברות, תשלומים ופעולות מעל לתקרת הסכום הראשונה שתיקבע ע"י התאגיד הבנקאי בהתאם לסעיף 60 (א) שלהלן;

(ב) הוספת ערוץ ושירות שלא למידע בלבד;

(ג) משיכת מזומנים מעמדה אוטומטית לשירות עצמי.

(ד) שינוי פרטי התקשרות או שם בעל החשבון בהתאם לסעיפים 58-57 שלהלן.

43. כאשר נדרשת הסכמה של כל השותפים בחשבון לביצוע פעולה או מתן הוראה לביצוע פעולה תידרש הסכמה כאמור גם במסגרת שירותי בנקאות בתקשורת.

44. על אף האמור בסעיף 43 לעיל, תאגיד בנקאי רשאי 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, בכפוף לקבלת אישור מאומת מהגורם המוסמך לכך בתאגיד.

פרק ה' – הגנה על לקוחות

ניטור חריגים ופעולות ברמת סיכון גבוהה

45. תאגיד בנקאי יישם מנגנון אוטומטי לזיהוי וניטור פעילות חריגה (אנומליות) בחשבונות של לקוחות ובפרט בפעולות ברמת סיכון גבוהה לצורך איתור של פעילות חשודה בזמן אמת.

46. באיתור הפעילות החריגה ייעשה שימוש גם בפילוח לפי קבוצות של לקוחות או חשבונות כגון: חשבונות מקוונים וחשבונות שצורפו לשירותי בנקאות בתקשורת באופן מקוון.

47. תאגיד בנקאי יעקוב אחר התפתחות שיטות הונאה ואיומים לבנקאות בתקשורת בארץ ובעולם ויעדכן במידת הצורך את מנגנון הניטור. לצורך כך, יעשה התאגיד הבנקאי שימוש במידע שהוא מקבל ממקורות פנימיים וחיצוניים (לרבות משטרה ומנגנוני בטחון וחברות לאבטחת מידע).

התראות ללקוחות

48. תאגיד בנקאי יתריע ללקוח על פעילות חריגה שזוהתה כאמור בסעיף 45 לעיל, על פעולות בהתאם לשיקול דעתו של התאגיד הבנקאי, ובכל מקרה על הפעולה המפורטת בסעיף 42(ב) לעיל. כמו כן ישקול נקיטת אמצעים באופן מידי כדוגמת השעיית עסקה או קבלת אשרור מהלקוח לעסקה.

49. ההתראות ובקשות האישורים ימסרו בערוץ אחר או במכשיר אחר מזה שבו בוצעה הפעולה, יכללו את פרטי העסקה המינימליים הנדרשים לצורך זיהויה, אך לא יכללו פרטים מזהים מלאים על החשבון או הלקוח או כרטיס החיוב.

50. בחירת הערוץ תיעשה תוך מתן משקל למהירות הנדרשת לקבלת ההתראה על ידי הלקוח, בהתאם לרמת הסיכון בעסקה, וכן לרמת אבטחת המידע הנדרשת בהתאם לרמת הרגישות של המידע המועבר, אלא אם כן בחר הלקוח ערוץ או מכשיר ספציפי לקבלת התראות ובקשת אישורים ובתנאי שסעיף 49 לעיל מתקיים.

51. בחשבון בו מספר שותפים ישלח התאגיד הבנקאי התראה על פעילות חריגה לכלל השותפים.

הדרכת לקוחות

52. תאגיד בנקאי יבהיר ללקוחותיו את הסיכונים העיקריים הכרוכים בקבלת שירותים בבנקאות בתקשורת ואת המלצותיו לנקיטת צעדי אבטחה סבירים בעת שימוש בשירותים אלה.

53. ההבהרה תינתן במגוון ערוצים, כגון: אתר הבנק, הודעות בעת כניסה לשירותי בנקאות בתקשורת, דוא"ל ודפי מידע.

54. התאגיד הבנקאי ינהל את הסיכון הכרוך באתרים או באפליקציות מתחזות וכאשר עולה חשד לתרמיות אחרות שמטרתן לגרום ללקוחות למסור מידע רגיש כגון: מספר חשבון, סיסמאות או מידע על כרטיס אשראי, לגורמים בלתי מורשים.
55. התעורר חשד לתרמית בשירותי בנקאות בתקשורת העלולים להשפיע על מספר רב של לקוחות בפרק זמן קצר, במקביל לפעילות התגובה להסרת האיום וצמצום הנזק הפוטנציאלי, ימסור התאגיד הבנקאי הודעה ללקוחותיו שנמצאים בסיכון וכן ישקול מסירת הודעה לציבור הרחב לפי העניין.

מוקד תמיכת לקוחות

56. תאגיד בנקאי יפעיל מוקד, שכולל מענה אנושי, לתמיכה בפעילות לקוחות בבנקאות בתקשורת.

פרק ו': בקרות בבנקאות בתקשורת

עדכון פרטי חשבון

57. שינוי פרטי התקשרות (כגון: מספר טלפון נייד, כתובת דואר אלקטרוני וכתובת פיזית), יתאפשר לאחר אימות באמצעות לפחות שני גורמי אימות.
58. עדכון שם בעל החשבון יתאפשר לאחר אימות באמצעות לפחות שני גורמי אימות והצגת העתק של מסמכי זיהוי ואימות, לפי העניין, הנדרשים לפי סעיף 3 לצו.
59. תאגיד בנקאי יבצע מעקב מוגבר אחר חשבונות בהם בוצעה פעילות חריגה שנוגעת לעדכון מרחוק של פרטי חשבון, למשך תקופה שתיקבע ובהתאם להערכת סיכונים.

העברות, תשלומים ופעולות אחרות

60. תאגיד בנקאי יקבע תקרות סכומים להעברות, תשלומים ופעולות אחרות למוטבים, כדלקמן:
    (א) תקרת סכום במסגרתה יידרש שימוש בגורם אימות אחד;
    (ב) תקרת סכום, אשר מתקרת הסכום כאמור בסעיף (א) לעיל ועד אליה, יידרש שימוש בשני גורמי אימות;
    (ג) מעל תקרת הסכום בסעיף (ב) לעיל, יידרש שימוש בטכנולוגיה המשלבת זיהוי ואימות של המשתמש, סודיות ושלמות הנתונים ומניעת הכחשה.
61. קביעת הסכומים כאמור, תתבסס על הערכת סיכונים שתתייחס, בין היתר, לזהות המוטב, סוג הלקוח ומאפייני פעילותו.
62. תאגיד בנקאי יקבע מדיניות ובקרות נאותות למזעור הסיכון להעברות בלתי מורשות, וביניהן, עבור לקוחות עסקיים אפשרות לבקרה המחייבת אישור של שני גורמים לביצוע כל העברה.

אבטחת ערוצי התקשורת

63. תאגיד בנקאי יעשה שימוש באלגוריתם הצפנה על מנת להגן על המידע של לקוחותיו העובר ברשתות חיצוניות לרבות האינטרנט ולמעט רשתות טלפוניה.

64. על אף האמור בסעיף 63 לעיל:

(א) תאגיד בנקאי רשאי לשלוח התראות ובקשות אישורים כאמור בסעיפים 48 ו- 49 לעיל, ללא שימוש באלגוריתם הצפנה.

(ב) לא יידרש שימוש באלגוריתם הצפנה בהעברת מידע בדואר אלקטרוני בנוגע לחשבון של בנק הפועל והמפוקח 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.

65. תאגיד בנקאי יבחן את הצורך ביישום אמצעים להבטחת השלמות של תוכן המסר ומניעת הכחשה בהעברת מידע.

פרק ז': בקרות במכשירים ובערוצים ספציפיים

פעילות לקוחות בדואר אלקטרוני

66. על אף האמור בסעיף 63 לעיל, בנוגע לקבלת מידע בדואר אלקטרוני מלקוחות, תאגיד בנקאי יביא בחשבון את הצורך בהצפנה, וכן את מידת הצורך בזיהוי חד משמעי של לקוח השולח דואר אלקטרוני, והכל בהתאמה לסוגי הפעילויות שנקבעו לשימוש באמצעות דואר אלקטרוני וסודיות המידע ובהתאם להערכת סיכונים.

משלוח מסרונים

67. העברת מידע באמצעות מסרונים לא תכלול פרטים מזהים מלאים על הלקוח ועל פרטי חשבון הלקוח (כגון: שם הלקוח, מספר חשבון הלקוח, מספר כרטיס חיוב).

שימוש במכשירים ניידים

68. תאגיד בנקאי יזהה ויעריך את הסיכונים הספציפיים הגלומים בשימוש במכשיר נייד לרבות אובדן או גניבה של המכשיר ויקבע אמצעי אבטחה לטיפול בסיכונים אלה.

69. תאגיד בנקאי ידריך את לקוחותיו לעניין השימוש במכשירים ניידים, לרבות הצורך באבטחה פיזית ולוגית שלהם והצורך בנעילת המכשיר. במסגרת זו יונחו הלקוחות כיצד לפעול במקרה של גניבה, אובדן או שימוש לרעה במכשיר נייד, ובמיוחד, כאשר המכשיר משמש לקבלת התראות ובקשות לאשור פעולות. תאגיד בנקאי ימסור ללקוחותיו מספר טלפון לדיווח במקרה הצורך, על מנת שהבנק יוכל לחסום שליחת התראות בערוץ זה.

70. בקרות נוספות ייקבעו על מנת לאפשר ללקוחות לקבל או ליצור סיסמה חד פעמית זמנית **(OTP)** משום שהאפקטיביות של **2FA** פוחתת כאשר אותו מכשיר משמש הן להתקשרות והן לקבלה או יצירה של **OTP**.

עמדות אוטומטיות לשירות עצמי

71. תאגיד בנקאי יישם אמצעי בקרה אשר יסייעו, בין היתר, למניעה ולזיהוי הונאות בעמדות אוטומטיות לשירות עצמי וביניהם:

(א) נתיב בקרה מספק לרבות תיעוד מתאים של המערכת;

(ב) תמיכה פונקציונלית מלאה לביצוע עסקאות בכרטיס חכם בעמדות אוטומטיות לשירות עצמי המשמשות למשיכת מזומן.

הוראות לביצוע פעולות בטלפון ע"י מענה אנושי

72. הוראות לביצוע פעולות בטלפון באמצעות מענה אנושי יירשמו ברשומות שיכללו, בין היתר, את מועד מתן ההוראה, פרטי הפקיד שקיבל את ההוראה וסימן מיוחד שההוראה ניתנה טלפונית.

פרק ח': ריכוז מידע

73. תאגיד בנקאי רשאי להציע ללקוחותיו שירות של "ריכוז מידע" (**Account Aggregation**) (להלן: השירות) בתנאים הבאים:

(א) השירות מוגבל לריכוז מידע בלבד.

(ב) לתאגיד הבנקאי ולעובדיו לא תהיה גישה למידע הלקוחות המתקבל מתאגידים אחרים (להלן: מידע הלקוחות), והם לא יעשו בו שימוש. לשם כך יישם התאגיד הבנקאי פתרונות טכנולוגיים שיתמכו בחסיון ובהגנה על המידע של לקוחותיהם, ויספק נתיב ביקורת לניסיונות גישה למידע, לרבות המידע על אמצעי הגישה לחשבונות התאגידים האחרים.

(ג) על אף האמור בסעיף (ב) לעיל, רשאי תאגיד בנקאי לעשות שימוש במידע הלקוחות בתנאי שקיבל מהלקוח אישור מפורש לעשות זאת ושהמידע יועבר לידיעת הלקוח בלבד.

(ד) תאגיד בנקאי יפעיל את השירות רק ביוזמת הלקוח לאחר שניתנה הסכמתו לכך.

(ה) תאגיד בנקאי ימחק מהמאגרים הרלוונטיים את המידע המאפשר גישה לחשבונות של לקוח המבקש להתנתק מהשירות.

(ו) תאגיד בנקאי לא יתנה את מתן השירות בהסכמת הלקוח לאמור בסעיף (ג) לעיל.

פרק ט': דיווחים ואישורים

נושאים שנדרש לגביהם דיווח

74. תאגיד בנקאי ידווח לפיקוח על הבנקים, בהתאם לסעיף 82 להוראת ניהול בנקאי תקין מספר 361 בנושא "ניהול הגנת הסייבר" על כל אירוע מהאירועים הבאים:

(א) אירוע או חשד לאירוע של תרמית בשירותי בנקאות בתקשורת, כדוגמת אתרים ואפליקציות מתחזים, הודעות פישינג, העלול להשפיע על מספר רב של לקוחות.

(ב) אירוע משמעותי הקשור לבנקאות בתקשורת לרבות ניסיונות מהותיים של חדירה וחדירות בפועל למערכות, הפסקת שירות של מערכות, והונאות.

נושאים שנדרש לגביהם אישור

75. תאגיד בנקאי המבקש לבצע פעילות מהותית חדשה במערכת הבנקאית בישראל בתחום הבנקאות בתקשורת, המובאת לאישור הדירקטוריון של הבנק, יפנה לפיקוח על הבנקים, תוך הצגת ניתוח מכלול הסיכונים והדרכים לניהולם, ויקבל את אישור הפיקוח על הבנקים לכך.

76. תאגיד בנקאי המבקש להציע ללקוחותיו שירותי ריכוז מידע יודיע מראש לפיקוח על הבנקים, תוך הצגת מכלול הסיכונים והדרכים שינקוט לניהולם, ויקבל את אישור הפיקוח על הבנקים לכך.