בנק ישראל
הפיקוח על הבנקים
תחום הסדרה

ירושלים, י״ז באלול תשס״ג
14 בספטמבר 2003
חוזר מס׳ ח-06-2118
(8557.doc)

לכבוד
התאגידים הבנקאיים

הנדון: **ניהול טכנולוגיית המידע**
(ניהול בנקאי תקין, הוראה מס׳ 357)

מבוא

1. טכנולוגיית המידע היא מרכיב מרכזי בתפעול ובניהול התקין של תאגיד בנקאי, לאור היותו של המידע, על כל היבטיו והשלכותיו, בעל השפעה מכרעת על יציבותו והתפתחותו של התאגיד הבנקאי. בשל כך, על הנהלת תאגיד בנקאי לייחס את החשיבות הראויה, הן בהיררכיה הניהולית והן במשאבים הכספיים ומשאבי האנוש הנחוצים, לניהול תקין של טכנולוגיית המידע.
לאחר התייעצות עם הוועדה המייעצת בעניינים הנוגעים לעסקי בנקאות קבעתי את ההוראה המצ״ב בדבר ניהול טכנולוגיית מידע. הוראה זו תואמת את העקרונות בתחום הבנקאות האלקטרונית, שפירסמה הועדה הבינלאומית לפיקוח על הבנקים (ועדת באזל) ביולי 2003.

תחולה

2. תחולת הוראה זו היא על תאגידים בנקאיים וכן על תאגידים כאמור בסעיפים 11(א)(3א) עד (3ג) ו-11(ב) לחוק הבנקאות (רישוי) התשמ״א-1981 **(סעיף 2 להוראה)**.

עיקרי ההוראה החדשה

3. דירקטוריון תאגיד בנקאי חויב בקיום דיון תקופתי וקביעת מדיניות ניהול טכנולוגיית המידע במסגרת מדיניות המחשוב של התאגיד הבנקאי. על המדיניות לכלול בין היתר התייחסות לאבטחת מידע, עקרונות גיבוי והתאוששות במצבים של תקלות ואסונות, מיקור חוץ, מדיניות פיתוח, לרבות על-ידי משתמשי קצה, ושימוש בטכנולוגיות חדשות במסגרת הבנקאות בתקשורת **(סעיף 3 להוראה)**.

דברי הסבר:

- הסעיף נותן ביטוי לאחריותו של הדירקטוריון על-ידי פירוט חובתו בעניין קביעת מדיניות ניהול טכנולוגיית המידע של התאגיד הבנקאי, אשר נקבעה בסעיף 6(יד) להוראת ניהול בנקאי תקין מס׳ 301 (דירקטוריון), על היבטיה השונים.

ת״ד 780 ירושלים 91007 פקסימיליה: 02-6552430 טלפון: 02-6552475

- יצוין כי יש לקיים דיון גם במקרים של שינויים מהותיים במערך טכנולוגיית המידע, וכן באירועים חריגים.

4. (א) הנהלת תאגיד בנקאי חויבה במינוי מנהל בעל הכשרה וניסיון מתאימים, אשר יישא באחריות למכלול נושאי טכנולוגיית המידע **(סעיף 4(א) להוראה)**.

דברי הסבר:

- לאור החשיבות והתלות של תאגיד בנקאי בטכנולוגיית המידע, ולאור הסיכונים הנגזרים מניהול לא תקין של תחום זה, נקבע שהאחראי על תחום זה על רבדיו השונים יכהן כחבר בהנהלת התאגיד הבנקאי או יהיה כפוף ישירות למנכ"ל התאגיד הבנקאי, ויהיה בעל הכשרה וכישורים הולמים.
- על מנהל טכנולוגיית המידע להיות ער לשינויים הטכנולוגיים, ולצורך בהתאמת המערך הקיים בעקבות שינויים אלה, לפי העניין.
- מנהל טכנולוגיית המידע יתרום למודעות בהקצאת המשאבים לתחום טכנולוגיית המידע ויאפשר ראייה מערכתית - בנקאית וטכנולוגית.

(ב) הנהלת תאגיד בנקאי חויבה בקיום דיון שנתי ביישום מדיניות ניהול טכנולוגיית המידע, וכן דיון מיוחד ביישום מדיניות אבטחת המידע על כל היבטיה **(סעיפים 4(ג) ו-4(ד) להוראה)**.

דברי הסבר:

התמורות התכופות בסביבה הטכנולוגית והשינויים במכלול הסיכונים, מחייבים התאמה של מדיניות טכנולוגיית המידע, יישומה ותקצובה, תוך הבחנה בין תוכניות ליישום בטווח הקצר לבין תוכניות שיישומן יתבצע בטווח הארוך. לפיכך נקבעה דרישה לקיום דיון שנתי.

מפאת חשיבות אבטחת המידע יוחד לה דיון נפרד.

5. תאגיד בנקאי חויב בקביעת נהלים מפורטים לכל שלב ולכל תהליך המטפלים בניהול, תפעול, אבטחה, גיבוי, שרידות ובקרה של טכנולוגיית המידע, והתאמתם באופן שוטף לשינויים בסביבה העסקית והטכנולוגית **(סעיף 5 להוראה)**.

דברי הסבר:

נהלים מפורטים המכסים את מגוון תחומי הפעילות של טכנולוגיות המידע חיוניים כדי להבטיח תמיכה שוטפת של מערך טכנולוגיה בפעילות התאגיד הבנקאי. מובהר, כי החובה לקבוע נהלים מפורטים מתייחסת גם לנושאים המפורטים בהוראה (כגון: בקרת גישה, קישור עובדים לאינטרנט, גיבוי והתאוששות וכד'). על תאגיד בנקאי לעדכן את הנהלים בסמוך להפעלת מערכת מידע חדשה, או בסמוך להכנסת שינויים מהותיים במערכת מידע קיימת.

6. (א) על תאגיד בנקאי לקיים תיעוד מתאים ועדכני למערך טכנולוגיית המידע שלו **(סעיף 6(א) להוראה)**.

(ב) תאגיד בנקאי יקיים נתיב ביקורת שיתבסס על רישום ממוכן (log) של עצם הגישה ושל פעולות ושאילתות המבוצעות במערכות המידע שלו, למעט מקרים של שאילתות של עובדים, בהם נדרש התאגיד הבנקאי לקיים נתיב ביקורת לפי שיקול דעתו, ועליו לקבוע פרק זמן לשמירת הרישומים כאמור **(סעיף 6(ב) להוראה)**.

(ג) על תאגיד בנקאי ליידע את לקוחותיו ועובדיו לגבי עצם קיומם של הליכי שמירה של פעולותיהם **(סעיף 6(ג) להוראה)**.

(ד) מצופה מתאגיד בנקאי שמערכות הניהול והבקרה יספקו התראות על פעילויות חיצוניות בלתי מורשות ועל פעילויות חריגות של המשתמשים לסוגיהם **(סעיף 6(ד) להוראה)**.

דברי הסבר:

תאגיד בנקאי יקיים נתיב ביקורת הולם של הפעילות המתבצעת בסביבה הממוחשבת. הרישום יכלול את עצם הכניסה למערכת (login) ואת הפעולות והשאילתות המבוצעות על ידי המשתמשים.

7. תאגיד בנקאי חויב לבצע הערכת סיכונים שתתעדכן באופן שוטף **(סעיפים 8(א) ו-8(ב) להוראה)** ובהתאם להערכת הסיכונים לנקוט באמצעים הנדרשים למזעור אפשרות פגיעה במערך טכנולוגיית המידע **(סעיף 8(ג) להוראה)**.

דברי הסבר:

הערכת סיכונים צריכה למפות את מערך טכנולוגיית המידע, ולדרג את הסיכונים השונים. הערכת סיכונים אינה פעולה חד פעמית הנעשית בנקודת זמן אחת, אלא פעילות מתמשכת, המתעדכנת בהתאם לשינויים בגורמי הסיכון השונים.

8. (א) הנהלת תאגיד בנקאי חויבה במינוי מנהל אבטחת מידע **(סעיף 4(ב) להוראה)**, תוך מניעת ניגוד עניינים וקביעת תחומי אחריותו, לרבות אלו המפורטים בהוראה, והעמדת המשאבים הדרושים למילוי תפקידו **(סעיף 9 להוראה)**.

דברי הסבר

- לאור חשיבות אבטחת המידע בסביבה טכנולוגית מורכבת ומשתנה, נקבעה פונקציית מטה שתישא באחריות הכוללת ליישום מדיניות אבטחת המידע בתאגיד הבנקאי. מנהל אבטחת מידע יהיה כפוף לחבר הנהלה של התאגיד הבנקאי, במטרה להביא למודעות של דרג ההנהלה את הנושאים הרלבנטיים בתחום זה ובשל משמעותו המרכזית בהתמודדות הולמת עם סיכוני אבטחת מידע.
- ממנהל אבטחת מידע נדרשת הכשרה מקצועית הולמת ומינוי באופן אישי, במטרה להבטיח אחריותו האישית לתחום אבטחת המידע.
- על הנהלת התאגיד הבנקאי למנוע ניגוד עניינים בעבודתו של מנהל אבטחת מידע, ובכלל זה לא ישמש כמנהל טכנולוגיית המידע של התאגיד הבנקאי.

(ב) תאגיד בנקאי חויב ביישום אמצעי אבטחה - פיזית ולוגית, למניעה, גילוי, תיקון ותיעוד של חשיפות במערך טכנולוגיית המידע, בהתאם להערכת הסיכונים ותוך התייחסות גם

להיבטים של זיהוי ואימות, סודיות ופרטיות, שלמות ומהימנות הנתונים ומניעת הכחשה **(סעיף 10 להוראה)**.

דברי הסבר:

השימוש במונחים מניעה וגילוי נעשה כאן במשמעותם הרחבה. במניעה הכוונה לכלול גם אמצעים כמו בקרת גישה פיזית, הקשחת מערכות הפעלה וכד'. בגילוי הכוונה לכלול גם אמצעים כמו סריקת לוגים (Log) כריית מידע (Data Mining) וכד'. בשל התכיפות בתמורות הטכנולוגיות והשפעתן על הסיכונים ועל אבטחת המידע, נדרש תאגיד בנקאי לעקוב אחר תמורות אלו ולהתאים אליהן את אבטחת המידע שהוא מיישם.

9. (א) תאגיד בנקאי יקיים סקר בטיחות של מערך טכנולוגיית המידע שלו, בהתאם להערכת הסיכונים. בסקר תוערך האפקטיביות של אמצעי ההגנה בהתייחס להערכת הסיכונים, ויוצעו דרכים לתיקון הליקויים שיימצאו. במערכות שהוגדרו על ידי התאגיד הבנקאי כבעלות סיכון גבוה, לרבות מערכות של בנקאות בתקשורת, יש לערוך סקר גם לפני הטמעת שינויים משמעותיים במערכות אלה, כאשר חלו שינויים משמעותיים בסביבה הטכנולוגית בה הן פועלות, ולקראת הכנסתן לשימוש של מערכות חדשות כאמור, ולפחות אחת ל-18 חודשים. תוצאות הסקר יכללו דוח מפורט על הממצאים וההמלצות, ותמצית ניהולית שתציג את עיקרי הדברים **(סעיף 11(א) להוראה)**.

(ב) מנהל אבטחת המידע ייזום ניסיונות חדירה מבוקרים למערך טכנולוגיית המידע של התאגיד הבנקאי לבחינת עמידותו בפני סיכונים פנימיים וחיצוניים. הניסיונות ייעשו בתדירות ההולמת את הסיכונים הספציפיים של המערכות, בהתאם להערכת הסיכונים **(סעיף 11(ב) להוראה)**.

(ג) נקבע, כי בביצוע סקרי הבטיחות וניסיונות החדירה המבוקרים, יישמרו עקרון אי התלות ומניעת ניגוד עניינים, ונדרשת מיומנות מקצועית מהמבצעים, והיותם חיצוניים לתאגיד הבנקאי. כמו כן נקבע, שהנהלת התאגיד הבנקאי תשלים את הדיון בממצאים תוך פרק זמן סביר לאחר מועד תחילת ביצוע הסקר וניסיונות החדירה המבוקרים, ותביא ממצאים מהותיים לידיעת הדירקטוריון או ועדה דירקטוריונית מתאימה. **(סעיפים 11(ג) ו-11(ד) להוראה)**.

דברי הסבר:

התמורות והשינויים במכלול הסיכונים, המורכבות הטכנולוגית של מערכות המידע, השילוב של טכנולוגיות מספקים שונים, הקישוריות שלהן למערכות ורשתות חיצוניות (אינטרנט וכד'), וההסתייעות בשירותי מיקור חוץ ודומיהם, חושפים את התאגיד הבנקאי למגוון סיכונים, המשתנים גם בהתאם לשינויים בסביבה הטכנולוגית ולפעילות התאגיד הבנקאי. כדי לאתר סיכונים אלו, וכדי לבחון את אפקטיביות אמצעי הבקרה והאבטחה המיושמים על-ידי התאגיד הבנקאי, נקבעה מסגרת של ביצוע סקר בטיחות ודרישה לביצוע ניסיונות חדירה מבוקרים למערך טכנולוגיית המידע של התאגיד הבנקאי, כמפורט בהוראה. על סקר הבטיחות וניסיונות החדירה להיעשות בתדירות סבירה, כמתחייב מהערכת הסיכונים.
תאגיד בנקאי המקיים ניסיונות חדירה מבוקרים בתדירות גבוהה, יכול לרכז ממצאים ממספר ניסיונות חדירה במסגרת של דיון אחד.

אמצעי האבטחה והבקרות, אשר נועדו למזער סיכונים במערכות המידע של התאגיד הבנקאי, מיושמים על-ידי גורמים שונים (עובדי התאגיד הבנקאי, ספקים חיצוניים וכו'). כדי להבטיח אי-תלות ומניעת ניגוד עניינים בביצוע סקר הסיכונים וניסיונות החדירה המבוקרים, נקבע כי הסקר וניסיונות החדירה יבוצעו על-ידי גורם חיצוני עצמאי ובלתי תלוי. יצויין, כי שימוש ברואה החשבון החיצוני של התאגיד הבנקאי לביצוע סקר בטיחות וניסיונות חדירה מבוקרים סותר את עקרון אי התלות ומניעת ניגוד העניינים.
ממצאים מהותיים יידונו בדירקטוריון או בועדה דירקטוריונית מתאימה, כמו ועדת המחשוב או ועדת הביקורת.

10. (א) נקבע, שתנאי מוקדם למתן גישה למערכות התאגיד הבנקאי יהיה זיהוי אישי של כל גורם בעל גישה. במקרים חריגים של ספקים ועובדים בהם לא ניתן לקיים את האמור, יינקטו אמצעים חלופיים מתאימים **(סעיף 12(א) להוראה)**. תאגיד בנקאי חויב בקביעת כללים וכלים לזיהוי ולמתן הרשאות לגורמים שונים לרכיבי טכנולוגיית המידע, תוך התחשבות ברמות הסיכון הנגזרות מטווח האחריות והסמכות של המשתמשים (על-פי סיווג לקבוצות), מהיישום עצמו, מרגישות המידע ומשאר רכיבי טכנולוגיית המידע **(סעיף 12(ב) להוראה)**.

דברי הסבר:
נקבעו עקרונות בסיסיים שעל התאגיד הבנקאי ליישם בכל הקשור לבקרת גישה. מובהר בזאת, כי יש לייחס חשיבות להשפעת כל אחד מהמאפיינים שהוזכרו בהוראה על רמות הסיכון. לפיכך, אפילו שינוי באחד מהמאפיינים (כגון: העברת יישום לסביבת עבודה שונה), יש בו כדי להשפיע על רמות הסיכון ולחייב התאמה של כללי הזיהוי ובקרת הגישה.
דוגמא למקרה חריג שבו לא ניתן ליישם זיהוי אישי, היא מפעילי מחשב המתחלפים תוך כדי פעולת המחשב, וזיהוי אישי יחייב השבתה של המחשב והפעלתו מחדש.

(ב) תאגיד בנקאי חויב בשימוש בטכניקות המשלבות זיהוי ואימות של המשתמש, סודיות ושלמות של הנתונים ומניעת הכחשה באמצעי הגישה למערכות מידע בעלות סיכון גבוה, ובכל מקרה של גישה מרחוק, למעט מקרים חריגים של גישה מרחוק של ספקים ונותני שירותים או גישה שלא מרחוק למערכות בסיכון גבוה בהתאם לשיקול דעתו של התאגיד הבנקאי, שבהם יישם התאגיד הבנקאי טכנולוגיה חלופית **(סעיף 12(ג) להוראה)**. כן נקבע, שעל תאגיד בנקאי לקבוע קריטריונים להפעלת מנגנון ניתוק התקשרות לשירות **(סעיף 12(ד) להוראה)**.

דברי הסבר:
הכוונה לשימוש בטכנולוגיות כמו סיסמאות מתחלפות, התקני PKI (Public Key Infrastructure) (שימוש במפתח הציבורי והפרטי, ללא חובת מעורבות של גורם מאשר (C.A)), זיהוי ביומטרי ואחרות.

בגישה שלא מרחוק ניתן לתאגיד הבנקאי שיקול דעת להפעיל טכנולוגיה חלופית, ובלבד שהנימוקים שבגינה קיבל התאגיד הבנקאי את ההחלטה יתועדו בכתב. ניתן להפעיל שיקול דעת כאמור גם על רמת מערכת או על מערכת שנועדה למגזר לקוחות ספציפי.

(ג) תאגיד בנקאי חויב לקיים הצפנה של נתונים במקרים מסוימים, כמפורט בהוראה **(סעיף 13 להוראה).**

דברי הסבר

ההוראה לא קבעה את חוזק ההצפנה, האחריות לכך חלה על התאגיד הבנקאי. כיום בבנקאות בתקשורת מצופה שימוש במפתח הצפנה של 128 ביט לפחות, כמקובל בעולם.

11. נקבעו כללים בנושא קישוריות תאגיד בנקאי לאינטרנט. בשלב זה מותרת קישוריות כאמור במקרים של מתן שירותי בנקאות בתקשורת וקישוריות של עובדי התאגיד הבנקאי תחת המגבלות המפורטות בהוראה. בנוסף, תאגיד בנקאי חויב בנקיטת אמצעים לאיתור התחזות של גורמים בלתי מורשים לאתר האינטרנט של התאגיד הבנקאי **(סעיף 14 להוראה)**.

דברי הסבר

- קישוריות תאגיד בנקאי לרשת האינטרנט חושפת אותו לסיכונים מיוחדים. עקב כך מתאפשרת קישוריות לאינטרנט מתחנות העבודה של עובדי התאגיד הבנקאי באמצעות רשת שקשורה אך ורק לאינטרנט (Stand Alone) ושאין עליה יישומים בנקאיים או מידע רגיש, או לחילופין באמצעות תצורה מאובטחת, אך ורק לצורכי גלישה ודואר אלקטרוני, ללא הורדת קבצים (למעט קבצים החיוניים לעצם ההתקשרות בין המחשבים ברמה התפעולית-טכנית). במקרה של הפרדה בין רשת התאגיד הבנקאי לבין רשת האינטרנט, באמצעים טכנולוגיים כדוגמת Terminal - Server, תתאפשר גם הורדת קבצים, תוך נקיטת אמצעי בקרה נאותים.
- קישוריות רשת התאגיד הבנקאי לרשת האינטרנט לכל שימוש אחר שאינו כלול בהוראה (לדוגמא, קישוריות לספקים) מחייבת היתר מהמפקח.
- נקבע כי על הנהלת תאגיד בנקאי לקבוע את השימושים המותרים לעובדי התאגיד הבנקאי באמצעות קישוריות לאינטרנט (כגון: החלטה האם לאפשר צירוף של קבצים (Attachment) אל התאגיד הבנקאי ומן התאגיד הבנקאי בעת שימוש בדואר אלקטרוני).
- נקבעו כללים מינימליים הכרחיים לאבטחת פעילות זו, לרבות לעניין מתן שירותי בנקאות בתקשורת כמפורט בפרק ז' בהוראה, ובכלל זה כלים להגנה על הרשת (מסנני תוכן, Antivirus וכו') וכלים ואמצעים לבקרה, זיהוי וניטור של חשיפות שונות במערכות (Vulnerability Assessment).

12. (א) הנהלת תאגיד בנקאי תקיים דיון אחת לתקופה בעקרונות הגיבוי וההתאוששות, תוך קביעה של התהליכים העסקיים החיוניים גם במצבי תקלות ואסונות, מערכות המידע הרלבנטיות לתפעולם ואופן תפעולן של מערכות אלה במצבים כאמור, והקמת אתר גיבוי לפחות עבור מערכות אלו. במסגרת הדיון התקופתי על ההנהלה לקבל החלטות בנושא הגיבוי השוטף והשקעות במתקני גיבוי והסדרי גיבוי אחרים **(סעיף 15 להוראה)**.

(ב) תאגיד בנקאי יקיים תכנית מפורטת להפעלת מערך טכנולוגיית המידע שלו במקרים של תקלות ואסונות, וכן יבצע ניסוי של כל הסדרי הגיבוי אחת לתקופה **(סעיפים 16(א)-(ב) להוראה)**.

(ג) תאגיד בנקאי חויב לאחסן גיבויי ציוד, תוכנה ומידע חיוניים במקום מרוחק ממקום אחסון המקור, במטרה למנוע פגיעה בו-זמנית בציוד, בתוכנה ובמידע המקוריים ובאתר הגיבוי **(סעיף 16(ג) להוראה)**.

דברי הסבר

- המשכיות ורציפות במתן שירותים בנקאיים סדירים תלויים במידה רבה ביכולת התאגיד הבנקאי להתאושש במהירות הנדרשת ממצבים של תקלות ואסונות, ולשם כך על התאגיד הבנקאי לקיים מערך גיבוי והתאוששות מסודר. הדבר אמור במיוחד לגבי תשתיות מחשוב כגון המחשב המרכזי של התאגיד הבנקאי ודומיו ולגבי מערכות בעלות רגישות מיוחדת כגון: חדרי עסקאות, שירותים מקוונים וכו'.
- על תוכנית החירום של התאגיד הבנקאי להיות מפורטת באופן שתקיף את מכלול הפעילויות שיש לבצע במקרים של תקלות ואסונות, לרבות מכלול ההיבטים המפורטים בסעיף 15 להוראה.

13. (א) נקבעו קווים מנחים להתקשרות תאגיד בנקאי עם גורמים חיצוניים לביצוע פעילויות ניהול, עיבוד ואחסון מידע **(סעיפים 17 ו-18 להוראה)**.

(ב) תאגיד בנקאי חויב בקבלת הסכמת המפקח על הבנקים מראש במקרים של מיקור חוץ של מערכות הליבה שלו, ואחסון מידע מכל סוג שהוא לגבי לקוחותיו במערכות שאינן בשליטתו הבלעדית **(סעיף 17(ב) להוראה)**.

דברי הסבר

מיקור חוץ חושף את התאגיד הבנקאי לסיכונים נוספים, אשר בעיקרם נובעים ממעורבותו של צד שלישי בתפעול מערכות המידע של התאגיד הבנקאי ולעיתים גם באחסון מידע בנקאי, דבר המקשה על השליטה והבקרה של התאגיד הבנקאי. ההוראה קובעת מספר כללים במטרה להפחית סיכונים אלו.

14. (א) נקבעו הוראות מיוחדות למתן שירותי בנקאות בתקשורת. הגדרת "בנקאות בתקשורת" שונתה, כך שהיא כוללת אחזור מידע על חשבונותיו של לקוח התאגיד הבנקאי או ביצוע פעולות או מתן הוראות לביצוע פעולות (גם אם בביצוע הפעולה מעורב פקיד) ביוזמת לקוח של התאגיד הבנקאי באמצעות מערכות תקשורת המקושרות למחשב התאגיד הבנקאי והעושות שימוש ברשת תקשורת (כגון: טלפוניה, אינטרנט, סלולרית) או שילוב בין רשתות תקשורת, למעט אחזור מידע או מתן הוראות לביצוע פעולות באמצעות פקס או באמצעות שיחה בה הלקוח ונציג התאגיד הבנקאי שומעים זה את זה, שעליה חלה הוראת ניהול בנקאי תקין מספר 435 (הוראות טלפוניות). יצוין כי אחזור מידע מתייחס גם למידע שנמסר ביוזמת התאגיד הבנקאי (כגון: מסירת יתרה באמצעות הודעת SMS למכשיר הסלולרי של הלקוח) ובלבד שהלקוח יזם את השירות באמצעות חתימה על הסכם הצטרפות מתאים **(סעיף 19(א) להוראה)**.

דברי הסבר

יודגש, כי גם כאשר מעורב פקיד בביצוע הפעולה, ההוראה חלה על כל החלקים שבהם נעשה שימוש בבנקאות בתקשורת. לדוגמא, בשליחת הוראה לביצוע פעולה בדואר אלקטרוני המבוצעת על ידי פקיד, ההוראה תחול עד לשלב שבו הפקיד נעשה מעורב.

(ב) הוגדרו ארבע רמות שירות של שירותי בנקאות בתקשורת. כן נקבע כי עדכון פרטים אישיים אינו כלול במסגרת רמות השירות של שירותי בנקאות בתקשורת **(סעיף 19(ב) להוראה)**.

דברי הסבר

הסיכונים להם חשופים התאגיד הבנקאי ולקוחותיו במסגרת מתן שירותי בנקאות בתקשורת, משתנים בהתאם לסוג השירות ורמתו, ולפיכך מחייבים קיומן של בקרות הולמות למזעור סיכונים אלה בהתאמה לרמת השירות. הגדרת רמות השירות נועדה לסייע לתאגיד הבנקאי בהערכת הסיכונים ובקביעת אמצעי ההגנה הננקטים למזעור סיכונים אלה, בהתאמה לרמת השירות.

ההוראה אינה מאפשרת עדכון פרטים אישיים כמו מספר ת.ז., שם, כתובת, מספר טלפון וכד' בבנקאות בתקשורת, וזאת משום העצמת הסיכון הכרוך בכך.

15. נקבע, שקבלת שירותי בנקאות בתקשורת מותנית בחתימה על הסכם. ההסכם ייחתם בסניף, ויאפשר ללקוח לבחור בנפרד כל שירות תקשורת המוצע על ידי התאגיד הבנקאי אשר הלקוח מבקש לקבלו, ושבמעמד חתימת ההסכם יימסר ללקוח אמצעי זיהוי ראשוני לצורך התחברות לשירותי בנקאות בתקשורת **(סעיף 20(א) להוראה)**. נקבעו כללים לכריתת הסכמים בתקשורת (הסכמים מקוונים) לצורך קבלת מידע, לחברות כרטיסי אשראי גם לצורך מתן אשראי במסגרת המאושרת ללקוח, וכן לצורך הרחבת שירותי בנקאות בתקשורת לערוצי תקשורת אחרים, כמפורט בהוראה **(סעיפים 20(ב) ו-20(ג) להוראה)**.

דברי הסבר

- ככלל, הסכם התקשרות בין התאגיד הבנקאי לבין הלקוח למתן שירותי בנקאות בתקשורת ייחתם בסניף.
- עם זאת, ההוראה מאפשרת קיום הסכם התקשרות מקוון בשני מקרים:

(1) הסכם מקוון לצורך קבלת מידע בלבד (רמת שירות (1)) ובכלל זה ריכוז מידע. לחברות כרטיסי אשראי הותר גם הסכם מקוון לצורך מתן אשראי, בתנאי שהאשראי ניתן עד לגובה מסגרת האשראי הבלתי מנוצלת של הלקוח, מפני שכרטיס האשראי משמש כאמצעי תשלום.

(2) הסכם מקוון באמצעות ערוץ תקשורת אליו הצטרף הלקוח בעבר בסניף, ובתנאי שההסכם עליו חתם הלקוח בסניף נחתם עד שלוש שנים לפני החתימה על ההסכם המקוון ושההסכם המקוון לא ירחיב את רמות השירות עליהם חתם הלקוח בסניף. הדבר אינו מתאפשר באמצעות מכשירי בנק אוטומטיים (ATM) או עמדות שירות.

- במסגרת הסדרת הליך זיהוי הלקוח לשם כריתת הסכם מקוון לקבלת שירותי בנקאות בתקשורת ברמת שירות (1), במטרה למזער את סיכון ההתחזות, נקבע כי העברת אמצעי הזיהוי הראשון (כגון: קוד המשתמש) והעברת אמצעי הזיהוי השני (הסיסמא הראשונית) תבוצענה בשתי דרכים שונות. מובהר, כי בכל מקרה של משלוח אחד מאמצעי הזיהוי האמורים באמצעות הדואר, המשלוח יבוצע על-פי הכתובת הרשומה בתאגיד הבנקאי (ולא על-פי כתובת שנמסרה לתאגיד הבנקאי בתקשורת).
- נקבע, כי על-מנת לכרות הסכם מקוון יש להציג את נוסח ההסכם במלואו על-גבי המסך בצורה בהירה וקריאה, ולאפשר את הדפסתו. לפיכך, בתנאים הקיימים כריתת הסכם כאמור באמצעות טלפון סלולרי אינה אפשרית.

16. (א) תאגיד בנקאי חויב להציג בפני לקוחותיו את התנאים, הסייגים והסיכונים הקשורים לשימוש בשירותי בנקאות בתקשורת הניתנים על-ידו, את עקרונות האבטחה הננקטים על-ידו על-מנת למזער סיכונים אלה, ולהמליץ בפני לקוחותיו על דרכי התגוננות בפני סיכונים אלה. **(סעיף 21 להוראה)**.

דברי הסבר

- בנושאי אבטחת המידע בהוראה זו, כוונתנו שהם יכללו בין היתר התייחסות לנקודות הבאות: מידע אודות זהות התאגיד הבנקאי, כתובת פיזית, וכתובות רלוונטיות המאפשרות יצירת קשר עימו; מה הלקוח יכול לצפות בתחום ההגנה על נתוניו בהקשרים של שימוש לרעה, אובדן, גישה לא מורשית, שינוי וחשיפה; מה הם עקרונות האבטחה שקבע התאגיד לשם אבטחה המידע של הלקוח והגנה עליו, ומה הסיכונים הכרוכים בהם; האם וכיצד משתמש האתר של התאגיד הבנקאי ב-Cookies ודומיהם.
- יצוין, כי במסגרת התנאים המוצגים ללקוח יש להבהיר גם את התנאים והסייגים בקשר לאפשרותו לבטל הוראת תשלום לטובת צד שלישי טרם ביצועה הסופי.
- מובהר בזה, כי עצם הצגת הסיכונים ללקוח, אינה מסירה מאחריותו של מי מהצדדים.

(ב) נקבעו כללים לבקרת גישה ומזעור סיכונים לעניין שירותי בנקאות בתקשורת, הכוללים קביעת אמצעי זיהוי אישיים לכל מורשה גישה בחשבון (כגון: מתן קוד משתמש וסיסמא אישיים לכל אחד מהמורשים לפעול בחשבון, בדומה למקובל בכרטיסי אשראי), והתאמה בין ההרשאות שיש ללקוח בחשבון לבין הרשאותיו לביצוע פעולות ואחזור מידע במסגרת שירותי בנקאות בתקשורת (כגון: ביצוע פעולה המצריכה יותר מחתימה אחת לא יתאפשר באמצעות שירותי בנקאות בתקשורת מבלי להבטיח את אישורה על-ידי הגורמים הרלבנטיים). כמו כן נקבעו אמצעי זיהוי למכשירי בנק אוטומטיים. **(סעיף 22 להוראה)**.

(ג) נקבעו כללים בסיסיים לעניין ניהול סיסמאות לזיהוי ואימות לקוחות, ובכללם אופן מסירת סיסמא ראשונית, החלפת סיסמא וביטולה, ושחרור סיסמא חסומה. **(סעיף 23 להוראה)**.

דברי הסבר

בעת הצטרפות לשירות יכול לקוח לקבל סיסמא ראשונית בסניף או באמצעות ערוץ תקשורת אחר שהלקוח הצטרף אליו קודם לכן (לדוגמא, לקוח שהצטרף לשירותי בנקאות בתקשורת באינטרנט יכול לקבל סיסמא ראשונית באמצעות ATM, IVR, עמדת שירות וכד'). נדגיש, כי בכל מקרה חתימת הסכם ההצטרפות תיעשה בסניף, ומסירת הסיסמא הראשונית תיעשה באופן אישי ותהיה חסויה.

ההוראה מרחיבה את האמצעים בהם ניתן לשחרר סיסמא חסומה, ומאפשרת לכלול בהם גם את הערוץ בו נחסם הלקוח, וכן אמצעים אחרים כדוגמת הטלפון. בכל מקרה, הזיהוי צריך להיות באמצעות פריטי זיהוי שנמסרו על ידי הלקוח מראש לעניין זה בעת חתימת ההסכם, או על פי פרטים שרשומים אצל התאגיד הבנקאי שלא עודכנו בתקשורת. יודגש, כי בכל מקרה הסיסמא תהיה חסויה ולכן לדוגמא, אין למסור את הסיסמא בטלפון.

כאשר הזיהוי בערוצי תקשורת שונים (כגון: ATM, IVR, אינטרנט, עמדת שירות וכד') נעשה באמצעות שני פריטים כאמור בסעיף 22(ב) להוראה, (לדוגמא, כרטיס חכם וסיסמא) יש הקלות בניהול הסיסמאות כאמור בהוראה.

(ד) נקבעו אמצעי בקרה שונים, וביניהם הצגת מועד ההתקשרות האחרון באותו ערוץ ככל שניתן, חובת קיום הליך לאישור כוונת לקוח לבצע פעולה, נקיטת אמצעים להגנה על מחשב/מכשיר אחר המשמשים את הלקוח מפני שימוש לא מורשה וחשיפת מידע על חשבונות הלקוח, ומתן אפשרות ללקוח לשמור ו/או להדפיס בזמן אמת תמונת מצב של הפעולה אותה ביקש לבצע. **(סעיף 24 להוראה)**.

דברי הסבר

ההוראה מחייבת הצגת מועד ההתקשרות האחרונה באותו ערוץ, למעט מקרים בהם הטכנולוגיה אינה מאפשרת יישום בקרה כאמור. מומלץ להציג ללקוח גם את הגישה האחרונה בערוצי תקשורת אחרים, ככל שהדבר אפשרי.

17. (א) נקבעו תקרות לעסקאות בתקשורת לטובת צד שלישי שלא על-פי רשימת מוטבים (רמת שירות (4)) **(סעיף 25(ג) להוראה)**.

(ב) במסגרת עסקאות בתקשורת לטובת צד שלישי נקבעו כללים לניהול רשימת מוטבים (רמת שירות (3)), אשר באמצעותה ניתן יהיה לבצע עסקאות לזכות המוטבים המופיעים בה בתקרות שנקבעו על ידי התאגיד ו/או הלקוח **(סעיף 26 להוראה)**.

דברי הסבר

- על-סמך הניסיון שהצטבר, הותאמו הכללים בנושא עסקאות לטובת צד שלישי ועודכנו הסכומים אשר נקבעו בסעיף 10 להוראה מס' 412 (שירותי בנקאות בתקשורת) (המבוטלת במסגרת חוזר זה), באופן המאפשר הקלה על פעילות הלקוחות במסגרת שירותי בנקאות בתקשורת מחד, מבלי לוותר על הבקרה הנחוצה מאידך.
- לעניין אופן עדכון רשימת המוטבים, במטרה להבטיח זיהוי קפדני של הלקוח נקבעו כללים שונים למקרה של עדכון המתבצע ביוזמת הלקוח ולמקרה בו התאגיד הבנקאי יוזם בקשה לאישור הרשימה המופיעה ברישומיו.

- בהתאם לאמור בסעיף 14 לעיל יודגש, כי סעיפים 25 ו-26 להוראה אינם חלים במקרה שבו עסקאות לטובת צד שלישי מבוצעות על ידי פקיד.

(ג) התקרות שקובעת ההוראה אינן חלות כאשר התאגיד הבנקאי משתמש בטכנולוגיה המשלבת זיהוי ואימות המשתמש, סודיות ושלמות הנתונים ומניעת הכחשה ברמת העסקה הבודדת **(סעיף 25(ד) להוראה)**.

דברי הסבר

קובץ המוטבים והתקרות נועדו למזער את הסיכונים ללקוח ולבנק, בעיקר בגין הכחשת עסקה. על כן, תאגיד בנקאי אשר מיישם טכנולוגיה המטפלת במניעת הכחשה ברמת העסקה הבודדת, זאת בנוסף לזיהוי, אימות והבטחת שלמות וסודיות הנתונים כאמור בסעיף 10(ב) לעיל, יוכל להשתמש בה ללא צורך בניהול רשימת מוטבים או במגבלות התקרות שקובעת ההוראה. במקרה זה על התאגיד הבנקאי האחריות לקבוע תקרות לביצוע עסקאות לטובת צד ג', גם בהתאם לדרישות הלקוח.

18. (א) הנהלת תאגיד בנקאי תקבע את השימושים ואת סוגי הפעילויות שמותר ללקוחות לבצע באמצעות דואר אלקטרוני, ותביא בחשבון את מידת הצורך בזיהוי חד משמעי של לקוח השולח דואר אלקטרוני, אימות והבטחת תוכן המסר, שמירה על סודיות ומניעת הכחשה, בהתאם לסוגי הפעילויות שהותרו **(סעיפים 27(א), ו-27(ב) להוראה)**.

(ב) נקבע כי הוראות לביצוע פעולות של לקוחות התאגיד הבנקאי באמצעות דואר אלקטרוני יינתנו תוך שימוש בטכנולוגיה לאימות זהותו של נותן ההוראה, מניעת הכחשה ושלמות וסודיות של המסר **(סעיף 27(ג) להוראה)**.

(ג) נקבע כי תאגיד בנקאי רשאי לשלוח באמצעות דואר אלקטרוני או באמצעות אתר התאגיד, הודעות אשר כללי הבנקאות (שירות ללקוח) (גילוי נאות ומסירת מסמכים), התשנ"ב - 1992, מאפשרים העברתן ללקוח באמצעות הדואר, ובלבד שיתקיימו התנאים המפורטים בהוראה **(סעיף 27(ד) להוראה)**.

דברי הסבר

- השימוש בדואר אלקטרוני כאמצעי תקשורת נוסף על אלו הקיימים (טלפון, פקס וכו') בין הלקוח לבין התאגיד הבנקאי, מחייב נקיטת אמצעים למזעור הסיכונים הרלבנטיים. ההוראה קובעת מספר כללים על מנת למזער סיכונים אלה.
- דוגמא לשימושים וסוגי פעילויות שהנהלת התאגיד הבנקאי תקבע האם ניתן ללקוח לבצע באמצעות דואר אלקטרוני היא מתן או אי-מתן הוראות ביצוע לשווקים מקוונים. בכל מקרה יודגש, כי הכוונה לדואר אלקטרוני במסר חופשי המחייב מעורבות פקיד הבנק לביצועה, ולא בדואר אלקטרוני המאפשר STP (Straight Through Processing – ביצוע ישיר ללא מעורבות פקיד הבנק).
- יצוין, כי בכל מקרה של הפסקת משלוח מסמכים אשר כללי גילוי נאות מאפשרים העברתם ללקוח באמצעות דואר אלקטרוני או באמצעות אתר התאגיד, אם בשל בקשת הלקוח להפסיק שירות זה ואם בשל קבלת אינדיקציה לפיה הדואר לא נתקבל או לא נפתח על-ידי הלקוח, יש לשלוח את המסמכים הרלבנטיים ללקוח בדואר רגיל.

19. (א) נקבעו כללים למתן שירותי ריכוז מידע (Account Aggregation) בין אם אלו מוצעים במודל "User Driven" (בדרך כלל באמצעות תוכנה המאוחסנת במחשב הלקוח) ובין אם במודל "הצד השלישי" (כאשר כאן "הצד השלישי" הוא התאגיד הבנקאי המציע שירות זה באמצעות שרת מחשב שבאחריותו). הלקוח מספק את פרטי החשבון, לרבות קוד וסיסמא, עבור החשבונות עליהם הוא מבקש לקבל שירות ריכוז מידע. במקרה הראשון נתוני הזיהוי והחשבונות מאוחסנים במחשב הלקוח, ובמקרה השני נתונים אלו מאוחסנים בשרת ייעודי של התאגיד הבנקאי ("הצד השלישי") **(סעיפים 28(א)-(ג) להוראה)**.

(ב) נקבע, כי תאגיד בנקאי המבקש לספק שירותי ריכוז מידע במודל "הצד השלישי" יעשה זאת באמצעות שרת ייעודי בניהולו ובאחריותו של התאגיד הבנקאי **(סעיף 28(ב))**.

(ג) בכל מקרה לא מתאפשר מתן שירותי ריכוז מידע באמצעות מיקור חוץ **(סעיף 17(ג) להוראה)**. כן נדרש תאגיד בנקאי המבקש לספק שירותי ריכוז מידע לקבל היתר מהמפקח על הבנקים **(סעיף 28(ד) להוראה)**.

(ד) התנאים שמעמידה ההוראה לתאגיד בנקאי המבקש להציע שירותים של ריכוז מידע המפורטים בסעיף 28(ג) נועדו, בין היתר, לשמור על חסיון המידע של הלקוח, בעיקר אם מידע זה מאוחסן בשרת התאגיד הבנקאי, להסדיר שימוש במידע המצרפי ולמנוע צבירת מידע על הלקוח מתאגידים בנקאיים אחרים בשרת התאגיד מציע השירות. בין היתר נקבע, כי תאגיד בנקאי יישם אמצעים טכנולוגיים להגנה מפני שימוש במידע זה.

דברי הסבר

כוונת סעיפים אלה היא להבטיח שתאגיד בנקאי, בין באמצעות טכנולוגיה ובין באמצעות עובדיו, לא ייגש ולא יעשה שימוש במידע שמעבירים תאגידים בנקאיים אחרים, זולת לפי ההנחיות הקשורות לביצוע ריכוז מידע. מובהר בזה, כי המונח מידע הלקוחות המצרפי, האמור בסעיף 28(ג)(3), כוונתו לנתוני הסך-הכל (אגרגט) ולא למידע פרטני או חתכים ממנו.

(ה) נקבעו התנאים על פיהם רשאי תאגיד בנקאי להמשיך ולשמור פרטים אישיים של משתמש בשירותי ריכוז מידע שאינו לקוח של התאגיד הבנקאי לאחר שזה ביקש להתנתק מהשירות **(סעיף 28(ג)(7) להוראה)**.

דברי הסבר

תאגיד בנקאי חייב לקבל הסכמת המשתמש מראש להמשך שימוש בפרטיו האישיים. יובהר, כי הכוונה לנתונים כגון שם, מען וטלפון, ובשום מקרה אין הכוונה לנתונים שנגזרים מהשימוש במידע שמקורו בחשבונותיו של הלקוח בבנקים אחרים.

20. נקבעו פעולות הטעונות הסכמה מוקדמת של המפקח, ביניהן: שימוש בערוצי תקשורת חדשים או מכשירים חדשים שלא היו בשימוש במערכת הבנקאית בישראל (כגון: אינטרנט בכבלים, אמצעי זיהוי חדשים כדוגמת זיהוי ביומטרי וכו'), אחסון מידע של התאגיד הבנקאי במערכות מידע של תאגיד מחוץ לקבוצה הבנקאית (במסגרת מיקור חוץ) וכו'. כן נקבעו

נושאים, אירועים ופעולות עליהם יש למסור דיווח למפקח, במועדים המפורטים בהוראה **(סעיף 30 להוראה)**.

דברי הסבר

במקרים בהם נדרשת הסכמה מראש של המפקח, מומלץ לפנות למפקח סמוך למועד ההחלטה, עוד לפני הביצוע, כדי שהעלויות הגבוהות הכרוכות בפיתוח המערכות והיישומים השונים לא ירדו לטמיון, אם המפקח לא יאשר אותם.

ביטול

21. הוראה מס' 357 (נהלים בדבר עיבוד נתונים אלקטרוני (ענ"א)) והוראה מס' 412 (שירותי בנקאות בתקשורת) בטלות עם תחילת הוראה זו.

תחילה

22. (א) תחילת הוראה זו היא ביום 1 בינואר 2004.

(ב) על אף האמור בסעיף קטן (א):

(1) תחילת האמור בסעיפים 6(א) ו-6(ד) היא לא יאוחר מיום 1.7.2004.

(2) תחילת האמור בסעיפים 22(ב) ו-22(ג) היא לא יאוחר מיום 31.12.2005.

(3) תחילת האמור בסעיפים 12(א)-(ג), 13(ב) ו-22(א), היא לא יאוחר מיום 31.12.2006.

הוראות מעבר

23. (א) כל ההיתרים שניתנו על ידי המפקח או מי מטעמו בקשר עם נושא הוראה זו בטלים. תאגיד בנקאי הסבור, שהיתרים שניתנו לו בעבר אינם מכוסים על ידי הוראה זו, יפנו בכתב תוך ציון ההיתר בו מדובר.

(ב) (1) תאגיד בנקאי, שקיים טרם פרסום חוזר זה פעילות הטעונה הסכמת המפקח כמפורט בסעיף 30(א) להוראה, יודיע על כך בכתב למפקח, תוך ציון הפסקה המתאימה לאותה פעילות.

(2) תוך 90 יום מתאריך חוזר זה, תאגיד בנקאי ידווח על מיקורי חוץ שניתנו לפני תחילת הוראה זו, אשר אילו ניתנו אחרי תחילת הוראה זו היו מחייבים הסכמת המפקח כאמור בסעיף 17 להוראה.

(3) הדיווח יישלח לממונה על המידע והדיווח בפיקוח על הבנקים.

(ג) האמור בסעיף 18 להוראה לא יחול על הסכמים, שנחתמו קודם לכניסת ההוראה לתוקף ושתחולתם עד ליום 31.7.2004. יש לפנות למפקח על הבנקים לגבי הסכמים כאמור, שתחולתם אחרי 31.7.2004.

(ד) חברות כרטיסי אשראי יחתימו את לקוחותיהם, אשר כבר פועלים בסביבת מענה טלפוני ממוחשב (IVR), על הסכם כאמור בסעיף 20(א) לעניין השימוש בערוץ זה בלבד, לכל המאוחר במועד חידוש כרטיס החיוב שברשותם.

עדכון הקובץ

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

להוציא עמוד	**להכניס עמוד**
300-2-4 [25] (11/02)	300-2-4 [26] (9/03)
357-1-3 [3] (8/97)	357-1-19 [4] (9/03)
412-1-4 [5] (8/97)	----------
499-10 [2] (11/02)	499-10 [3] (9/03)

בכבוד רב,

יואב להמן

המפקח על הבנקים