

יום רביעי 29 מרץ 2017

אל: חברי הנהלת הרשות

הנדון: היערכות לתום תקופת המבחן- יח' אבטחת מידע

מצי"ב תוכנית העבודה ליישום לאור החוק, התקנות והצו לאחר תקופת המבחן של יח' אבטחת מידע

סעיפים מהחוק ומימושים

4(ב) האמצעים והנתונים המוצפנים שהועברו למרכז הנפקה לפי הוראות סעיף 3(ג) לא ייאגרו באופן ממוחשב, מעבר לנדרש לצורך הנפקת מסמך זיהוי והם יימחקו באופן אוטומטי מיד לאחר הנפקתו.

היערכות:

1. אין לאגור נתונים ביומטרים של אזרחים בכל מקום שהוא במערכת או במרכזי הנפקה. מידע ביומטרי ישמר במערכת בהתאם לדרישות החוק עד אשר הונפק מסמך הזיהוי ואז ימחק לצמיתות.
2. **XXX**
3. אחת לשנה תיערך ביקורת ברשת **XXX** לוודוא אי שמירת הנתונים במערכי **XXX**

4(ג) על מרכז הנפקה יחולו ההוראות לעניין סודיות, שמירת מידע, אבטחת מידע והגנת הפרטיות החלות על משרד הפנים לפי חוק זה, לפי חוק להסדרת הביטחון ולפי כל דין אחר, והכל בהתאמות שקבע השר בתקנות, באישור ועדת הכנסת המשותפת ליישומים ביומטריים.

היערכות: אחת לשנתיים תיערך ביקורת אבטחת מידע במרכזי **XX**

5(א) עובד משרד הפנים או מרכז הנפקה שקיבל אמצעים או נתונים ביומטריים לפי הוראות סימן זה לא יעבירם לכל גורם אחר, על אף האמור בכל דין, אלא לפי הוראות סימן זה.

היערכות:

יצאה הנחייה לאנשי אגף מרשם ומעמד הרלוונטים, אנשי **XX** ואנשי **XX** יבוצע ניטור במערכות **XXX**

6(ו) אמצעי זיהוי ביומטריים שניטלו לפי הוראות סעיף זה ונתוני זיהוי ביומטריים שהופקו מהם, לא ייאגרו באופן ממוחשב, מעבר לנדרש לצורך השוואתם מול האמצעים או הנתונים הביומטריים שבמסמך הזיהוי, והם יימחקו אוטומטית מיד לאחר קבלת תוצאת ההשוואה, אלא אם כן נדרשת השוואתם לאמצעים או לנתונים

ביומטריים שבמאגר הביומטרי לפי סעיף 7(א)(2).
היערכות XXX

9(א) נטילת אמצעי זיהוי ביומטריים, הפקת נתוני זיהוי ביומטריים והשוואתם לאמצעים או לנתונים ביומטריים שבמסמך זיהוי או במאגר הביומטרי, לפי הוראות פרק זה, יבוצעו בדרך ובמקום שיבטיחו שמירה על כבוד האדם ועל פרטיותו וימנעו פגיעה בהם במידה העולה על הנדרש.
היערכות במסגרת הביקורות בלשכות נושא זה מבוקר

9(ב) מי שהוקנתה לו סמכות נטילה, הפקה או השוואה לפי הוראות פרק זה, לא יעשה שימוש בסמכותו אלא לאחר שעבר הכשרה מתאימה; הכשרה לפי פסקה זו תתייחס, בין השאר, לאופן הנטילה, ההפקה וההשוואה לפי פרק זה, לאופן הטיפול באמצעים או בנתונים הביומטריים שניטלו או שהופקו כאמור ולסיכונים הנובעים מאי-אבטחת המידע, והכל תוך הקפדה על שמירת כבודו של מי שנוטלים ממנו אמצעי זיהוי ביומטריים ועל פרטיותו.
היערכות במסגרת הדרכות בקורס רע"נים וההדרכות השוטפות בלשכות הנושא נלמד לעומקו

24(א) אדם שהגיע לידיו, תוך כדי מילוי תפקידו או במהלך עבודתו, אמצעי זיהוי ביומטריים שניטלו לפי חוק זה, נתוני זיהוי ביומטריים שהופקו מהם, תוצאות זיהוי או תמונות פנים באיכות פחותה, וכן אדם שהגיע לידיו מידע אחר החסוי לפי חוק זה, לא ימסור ולא יגלה אותם לאחר ולא יעשה בהם כל שימוש, אלא לפי חוק זה ולצורך ביצוע תפקידו.
היערכות: יצאה הנחייה לאנשי אגף מרשם ומעמד הרלוונטים, אנשי XX ואנשי XX נערכת בקרה טכנולוגית על ידי XXX

24(ב) מידע שהועבר לפי הוראות חוק זה, למעט תוצאת זיהוי שהועברה מהרשות לעובד משרד הפנים לפי סעיף 14, לא יאגר באופן ממוחשב, מעבר לנדרש לצורך השימוש שלו הוא נועד, והוא יימחק מיד בתום השימוש בו.
היערכות: יצאה הנחייה לאנשי אגף מרשם ומעמד הרלוונטים, אנשי XX ואנשי XX נערכת בקרה טכנולוגית על ידי XXX

24(ב) מידע שהועבר לפי הוראות חוק זה, למעט תוצאת זיהוי שהועברה מהרשות לעובד משרד הפנים לפי סעיף 14, לא יאגר באופן ממוחשב, מעבר לנדרש לצורך השימוש שלו הוא נועד, והוא יימחק מיד בתום השימוש בו.
היערכות: יצאה הנחייה לאנשי אגף מרשם ומעמד הרלוונטים, אנשי XX ואנשי XX

סעיפים מהתקנות ומימושים

10(א) אמצעים או נתונים ביומטריים שהתקיימו בהם דרישות האיכות המפורטות בתקנה 5, או החריג האמור בתקנה 6(ג), יוצפנו באופן מיידי וממוכן בעמדת המחשב שבה בוצעה נטילת האמצעים האמורים, באמצעות מפתחות הצפנה אקראיים שאינם ידועים לעובד רשות האוכלוסין ואינם נמצאים בשליטתו, באופן שאישר ראש הרשות הממלכתית לאבטחת מידע בשירות הביטחון הכללי או מי מטעמו.

היערכות:
 תבוצע בדיקה XXXXXXXXXXXXXXXXXXXXXXX אחת לשנה אחר ביצוע ההנחיה

10 (ב) לצורך ביצוע הצפנה של אמצעים ונתונים ביומטריים, ייעשה שימוש באלגוריתם והליך הצפנה שאישר מראש ראש הרשות הממלכתית לאבטחת מידע בשירות הביטחון הכללי או מי מטעמו.
היערכות:
 אושר

10 (ג) מפתחות הפענוח יישמרו בידי הרשות ומרכז ההנפקה בלבד, וייעשה בהם שימוש לצורך מילוי תפקידם לפי תקנות אלה בלבד; ראש הרשות יקבע דרישות אבטחת מידע לגבי מפתחות אלה.
היערכות:
 XXXXXXXXXXXXXXX

10 (ד) אמצעים ביומטריים שניטלו מתושב ונתונים ביומטריים שהופקו מהם ושאינם מוצפנים, יימחקו באופן אוטומטי ומייד מעמדת המחשב שבה בוצעה הנטילה לאחר ביצוע ההצפנה לפי תקנת משנה (א), ולא יהיה ניתן לשחזרם בעמדה זו.
היערכות:
 XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
 XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

11 (ה) הנתונים המוצפנים יימחקו מכל מקום שבו נשמרו במהלך ההעברה, לכל המאוחר עם קבלת אישור ממרכז ההנפקה ומהרשות בדבר קבלת הנתונים.
היערכות:
 XXXXXXXXXXXXXXXXXXXXXXX

12 לצורך שמירה על רמת אבטחה נאותה, יבצע ממונה על אבטחת מידע לפי סעיף 17 ב לחוק הגנת הפרטיות, או מי מטעמו, בדיקה מדגמית במחשבי רשות האוכלוסין ובמרכז ההנפקה, להבטיח כי מתקיימת מחיקה של קבצי מחשב הכוללים אמצעים או נתונים ביומטריים, שנשמרו באופן זמני באותם מחשבים לצורך הנפקת מסמכי זיהוי לפי החוק.
היערכות:
 XXXXXXXXXXXXXXXXXXXXXXX

15 מי שהוקנתה לו סמכות נטילה, הפקה או השוואה לפי הוראות פרק ג' לחוק, יידרש לעבור הכשרה בנושאים שלהלן, בטרם יעשה שימוש בסמכות שהוקנתה לו:
 (1) תהליך נטילת אמצעי זיהוי ביומטריים, הפקת נתוני זיהוי ביומטריים והשוואת האמצעים או הנתונים כאמור לאמצעים או לנתונים הביומטריים הכלולים במסמך הזיהוי של אותו אדם;
 (2) אבטחת מידע והגנת הפרטיות;
 (3) המאגר הביומטרי;
 (4) עקרונות החוק והתקנות והכרת נוהלי עבודה חדשים;
 (5) שמירה על כבוד האדם ומתן שירות לאוכלוסיות בעלות מאפיינים מיוחדים;
 (6) הדרכה מעשית-תפעולית;
 (7) בתקופת המבחן לפי סעיף 41(1) לחוק – עקרונות תקופת המבחן.

היערכות

במסגרת הדרכות בקורס רע"ניים וההדרכות השוטפות בלשכות הנושא נלמד לעומקו

סעיפים מהצו ומימושם

10א (א) רשות האוכלוסין והרשות יוודאו טרם תחילת תקופת המבחן כי כל מערכי הטכנולוגיה, התפעול והמערך הביזמטרי למימוש מטרות תקופת המבחן עומדים בתקנים וברמת האבטחה של הרשות הממלכתית לאבטחת מידע במשרד ראש הממשלה ושל נוהלי רשות האוכלוסין והרשות.

(ב) רמת הגדרת סיווג המערכות המפורטות בסעיף קטן (א) לא תפחת מההגדרות שנקבעו בתחילת תקופת המבחן עד תום תקופת המבחן.

(ג) רשות האוכלוסין והרשות יבצעו מבדקי אבטחה באופן שייקבע בפרוטוקול המבחן או על בסיס השיטות המקובלות בתחום ניהול סיכונים ומבדקי אבטחה.

(ד) רשות האוכלוסין והרשות יבצעו סקר סיכונים אחד לפחות במהלך תקופת המבחן.

(ה) מבדקי האבטחה וסקר הסיכונים יבוצעו באמצעות גוף חיצוני שעיסוקו המרכזי באבטחת מידע ומבדקי אבטחה, ושעובדיו עברו בדיקת התאמה ביטחונית כמשמעותה בסעיף 7 לחוק שירות הביטחון הכללי.

(ו) מדדים לפי סעיף זה, לרבות לעניין בחינת מבדקי האבטחה וכן קביעת סקר הסיכונים, ייבחנו ביחס לתרחישי אירועים שבהם לפי קביעת הרשות הממלכתית לאבטחת מידע במשרד ראש הממשלה עלול להיגרם נזק חמור ומתמשך לביטחון המדינה, וכן ביחס לתרחישי אירועים הקשורים להגדרת רמת סיווג ורגישות המערכות הנדרשת למטרות תקופת המבחן, לרבות פגיעה בזכות התושבים לפרטיות.

היערכות:

כלל הנושאים יבדקו אחת XXXXXXXXXX במסגרת סקר סיכונים

10א (א) רשות האוכלוסין והרשות יוודאו טרם תחילת תקופת המבחן כי כל מערכי הטכנולוגיה, התפעול והמערך הביזמטרי למימוש מטרות תקופת המבחן עומדים בתקנים וברמת האבטחה של הרשות הממלכתית לאבטחת מידע במשרד ראש הממשלה ושל נוהלי רשות האוכלוסין והרשות.

(ב) רמת הגדרת סיווג המערכות המפורטות בסעיף קטן (א) לא תפחת מההגדרות שנקבעו בתחילת תקופת המבחן עד תום תקופת המבחן.

(ג) רשות האוכלוסין והרשות יבצעו מבדקי אבטחה באופן שייקבע בפרוטוקול המבחן או על בסיס השיטות המקובלות בתחום ניהול סיכונים ומבדקי אבטחה.

(ד) רשות האוכלוסין והרשות יבצעו סקר סיכונים אחד לפחות במהלך תקופת המבחן.

(ה) מבדקי האבטחה וסקר הסיכונים יבוצעו באמצעות גוף חיצוני שעיסוקו המרכזי באבטחת מידע ומבדקי אבטחה, ושעובדיו עברו בדיקת התאמה ביטחונית כמשמעותה בסעיף 7 לחוק שירות הביטחון הכללי.

(ו) מדדים לפי סעיף זה, לרבות לעניין בחינת מבדקי האבטחה וכן קביעת סקר הסיכונים, ייבחנו ביחס לתרחישי אירועים שבהם לפי קביעת הרשות הממלכתית לאבטחת מידע במשרד ראש הממשלה עלול להיגרם נזק חמור ומתמשך לביטחון המדינה, וכן ביחס לתרחישי אירועים הקשורים להגדרת רמת סיווג ורגישות המערכות הנדרשת למטרות תקופת המבחן, לרבות פגיעה בזכות התושבים לפרטיות.

היערכות:

כלל הנושאים יבדקו אחת XXXXXXXXXXXX במסגרת סקר סיכונים

בברכה,
עידו תלמי
מנהל אבטחת מידע
רשות האוכלוסין וההגירה