ריכוז תקנות אבטחת מידע - חוק הגנת הפרטיות

סעיף 1: רישום המאגר

רישום המאגר בפנקס מאגרי המידע של הרשות להגנת הפרטיות.

סעיף 2: מסמכי מאגרי מידע

תקנה 2א

כל בעל מאגר יגדיר וירשום במסמך את ההגדרות הנדרשות עפ"י תקנה 2א' בתקנות הגנת הפרטיות.

הסבר משלים: הארגון יחזיק עבור כל מאגר רשום מסמך המכיל:

- תיאור כללי של פעולות האיסוף והשימוש במידע;
- תיאור מטרות השימוש במידע;
- סוגי המידע השונים הכלולים במאגר המידע;
- פרטים על העברת מאגר המידע, או חלק מהותי ממנו אל מחוץ לגבולות המדינה או שימוש במידע מחוץ לגבולות המדינה, מטרת ההעברה, ארץ היעד, אופן ההעברה וזהות הנעבר;
- פעולות עיבוד מידע באמצעות מחזיק;
- הסיכונים העיקריים של פגיעה באבטחת המידע, ואופן ההתמודדות עמם;
- שמו של מנהל מאגר המידע, של מחזיק המאגר ושל הממונה על אבטחת מידע בו, אם מונה כזה.

הערות: את מסמך ההגדרות נדרש לעדכן אחת לשנה או אם נעשה שינוי משמעותי באחד הפרמטרים לעיל:

- אם נעשו שינויים טכנולוגיים רלבנטיים;
- אם נעשו שינויים ארגוניים רלוונטיים;
- אם אירע אירוע אבטחה.

סעיף 3: תאימות

תקנה 2

קיום מדיניות אבטחת מידע והגנה בסייבר ארגונית.

הסבר משלים: מסמך המדיניות יכיל בתוכו פרק "הגנת הפרטיות" אשר ייתן מענה מלא לדרישות.

הערות: על המדיניות לכלול הגדרות ברורות לגבי הוצאת מידע אל מחוץ לגבולות הארגון ואופן הוצאת המידע.

סעיף 4: תמיכה במדיניות הגנת הסייבר

תקנה 2ב', 2ג'

ועדת ההיגוי תאשר את מדיניות אבטחת המידע והגנת הסייבר אחת לשנה ותקצה משאבים נדרשים לטובת מימושה.

הסבר משלים:

- אחת לשנה תוצג מדיניות אבטחת המידע והגנת בסייבר הארגונית, כנגזרת ממפת סיכוני הסייבר של הארגון.
- ועדת ההיגוי לסייבר תאשר את מפת הסיכונים ואת המדיניות הנגזרת ממנה לרבות עמידה בתקנות הגנת הפרטיות.

סעיף 5: סיווג מידע

תקנה 2ב' (3)

על הארגון לכתוב וליישם מדיניות לסיווג מידע ארגוני ונהלי יישום לעובדי הארגון לצורך תיוג המידע.

הסבר משלים: על מדיניות סיווג לכלול הגדרות ברורת כיצד ואיך לסווג כל סוג מידע שאופיין כמו כן יש להוסיף נוהל המנחה כיצד יש לטפל בכל אחד מסיווגי המידע.

סעיף 6: עקרון צמצום מידע וצמידות מטרה

תקנה 2 ג'

ניהול מידע data minimization.

הסבר משלים: מנהל מאגר מידע יבחן, אחת לשנה, אם אין המידע שהוא שומר במאגר רב מן הנדרש למטרות המאגר.

סעיף 7: תאימות

תקנה 3, 3(1), 3(4), 3(5), 3(6)

ממונה אבטחת מידע לתחום הגנת הפרטיות

הסבר משלים:

- חלה חובה למנות ממונה על אבטחת מידע, המינוי ייצא בכתב מינוי מטעם מנכ"ל הארגון.
- ממונה אבטחה יהיה כפוף ישירות למנהל מאגר המידע .
- כתב מינוי מנהל אבטחת המידע יגדיר את כלל הסמכויות, האחריות והמשימות אשר נדרש למלא הממונה.
- נוהל אבטחת מידע להגנת הפרטיות - נוהל העומד בתאימות לתפיסת האבטחה בארגון.

סעיף 8: תאימות

תיקון 13 לחוק הגנת הפרטיות

ממונה הגנת הפרטיות

הסבר משלים:

חובת מינוי ממונה הגנת הפרטיות בגופים ציבוריים ובכל ארגון שעיסוקו העיקרי כולל עיבוד מידע אישי רגיש בהיקף ניכר, כמו גם בכל ארגון שפעילותו כרוכה במעקב או התחקות שיטתית אחר אנשים בהיקף ניכר. תפקידו של ממונה הגנת הפרטיות בארגון הוא לפעול להבטחת קיום הוראות חוק הגנת הפרטיות ותקנותיו ולקידום השמירה על הפרטיות גם מעבר לדרישות החוק.

סעיף 9 : אחריות וסמכות

תקנה 3

לוח סמכויות והגדרת תפקידים במערך הגנת הסייבר.

הסבר משלים: קיימות הגדרות תפקיד ברורות הכוללת גם הגדרת אחריות וסמכות.

סעיף 10 : נוהל

תקנה 3(2), 4(א,ג)

הממונה על אבטחה יכין נוהל אבטחת מידע ויביאו לאישור ההנהלה בארגון

הסבר משלים: הנוהל צריך לכלול לפחות את הנושאים הבאים:

1. הוראות בעניין האבטחה הפיזית והסביבתית של אתרי המאגר (כאמור בתקנה 6)
2. הרשאות גישה למאגרי המידע ולמערכות המאגר (בהתאם לתקנה 8)
3. תיאור של אמצעים שמטרתם הגנה על מערכות המאגר ואופן הפעלתם לצורך כך.
4. הוראות למורשי הגישה למאגר המידע ולמערכות המאגר לצורך הגנה על המידע במאגר.
5. הסיכונים שחשוף להם המידע שבמאגר.
6. אופן התמודדות עם אירועי אבטחת מידע כאמור בתקנה 11 .
7. הוראות לעניין ניהול של התקנים ניידים ושימוש בהם כאמור בתקנה 12
8. אמצעי הזיהוי והאימות לגישה למאגר ולמערכות המאגר, בהתאם לתקנה 9
9. אופן הבקרה על השימוש במאגר המידע, ובכלל זה תיעוד הגישה למערכות המאגר כאמור בתקנה 10
10. הוראות לעניין עריכת ביקורות תקופתיות לווידוא קיומם ותקינותם של אמצעי האבטחה
11. כאמור בתקנה 16
12. הוראות לעניין גיבוי הנתונים האמורים בתקנה 18 (א1)
13. הוראות לעניין אופן ביצוע פעולות פיתוח במאגר ותיעודן, ובכלל זה אופן הגישה של אנשי הפיתוח לנתונים במאגר.

הערות: אחת לשנה יש לבחון את הצורך בעדכון הנוהל :

- אם נעשו שינויים מהותיים במערכות המאגר או בתהליכי עיבוד המידע ;
- אם נודע על סיכונים טכנולוגיים חדשים הנוגעים למערכות המאגר.

סעיף 12 : תכנון

תקנה 3(3)

תוכנית עבודה

הסבר משלים:

- קיום תוכנית עבודה מסודרת הכוללת גם תקצוב הולם.
- תוכנית העבודה תאגד את כלל תוכניות העבודה בכל תחומי ההגנה בסייבר, לרבות הגנה על מאגרי מידע.

סעיף 13 : מיפוי מערכות המאגר

תקנה 5 א'

מסמך מעודכן של מבנה מאגר המידע וכן רשימת מצאי מעודכנת של מערכות המאגר.

הסבר משלים : המסמך יכלול את הפרטים הבאים :

1. תשתיות ומערכות חומרה, סוגי רכיבי תקשורת ואבטחת מידע.
2. מערכות התוכנה המשמשות להפעלת מאגר המידע, לניהול המאגר ולתחזוקתו, לתמיכה בפעילותו, לניטורו ולאבטחתו.
3. תוכנות וממשקים המשמשים לתקשורת אל מערכות המאגר ומהן.
4. תרשים הרשת שבה פועל המאגר, הכולל תיאור הקשרים בין רכיבי המערכת השונים ומיקומם הפיזי של הרכיבים.
5. תאריך העדכון האחרון של המסמך ושל רשימת המצאי.

הערות :

- הכנת המסמך באחריות של בעל מאגר המידע.
- ארגון בעל כמה מאגרי מידע, רשאי לקבוע את רשימת המצאי במסמך אחד לגבי כל מאגרי המידע, המצויים באותה רמת אבטחה.

סעיף 14 : מבדקי חדירה

תקנה 5ג'-ד'

יש לבצע מבדקי חדירות למערכות המאגר אחת ל-18 חודשים לפחות, על מנת לבחון עמידותן בפני סיכונים פנימיים וחיצוניים.

הסבר משלים : חלה חובה, במאגר מידע שחלה עליו רמת האבטחה הגבוהה.

הבהרה :

על אילו מאגרים חלה רמת האבטחה הבינונית ?

1. מאגר מידע שמטרתו העיקרית היא איסוף מידע לצורך מסירתו לאחר כדרך עיסוק, לרבות שירותי דיוור ישיר.
2. מאגר מידע שבעליו הוא גוף ציבורי (ארגוני הממשלה, רשות מקומית וכו').
3. מאגר מידע הכולל מידע על צנעת חייו האישיים של אדם, מידע רפואי, מידע גנטי, מידע על דעות פוליטיות, מידע על עבר פלילי, נתוני תקשורת, מידע ביומטרי, מידע על נכסיו של אדם וכו', הרגלי צריכה.

על אילו מאגרים חלה רמת האבטחה הגבוהה ?

מדובר במאגרי מידע שחלה עליהם רמת האבטחה הבינונית, שיש בהם מידע על אודות 100,000 אנשים ומעלה או שמספר בעלי ההרשאה בו עולה על 100.

סעיף 15 : סריקות אבטחה

תקנה 5ג'-ד'

יש לבצע סריקת פגיעויות באופן שוטף ובהתאם לתהליך ניהול הפגיעויות הארגוני, באמצעות כלי יעודי למטרה זו על מערכות המידע של הארגון (פנימיות וחיצוניות).

הסבר משלים : ניתן לממש באמצעות התקנה של כלי לסריקת פגיעויות ותזמון סריקות - vulnerability assessment.

סעיף 16 : ניהול והערכת סיכונים

תקנה 5ג'-ד'

יש לערוך סקר סיכונים (אחת ל-18 חודשים לפחות).

הסבר משלים : חלה חובה, במאגר מידע שחלה עליו רמת האבטחה הגבוהה

1. מטרת תהליך הערכת הסיכונים הינה לספק מפה עדכנית של סיכוני הסייבר בפועל (סיכונים שיוריים) במטרה להגדיר תוכנית לטיפול בסיכונים.
2. יש ידון בתוצאות הסקר ולפעול לתיקון הליקויים, אם התגלו.

סעיף 17 : אבטחה פיזית

תקנה 6 א'

שמירה פיזית של תשתיות ומערכות החומרה המשמשות את המאגר, במקום מוגן המונע כניסה אליו ללא הרשאה. זאת לאור העובדה כי הגדרות הליבה של המערכת ואמצעי ההגנה הלוגיים שלה כפופים לסיכון של שינוי ועדכון באמצעות גישה פיזית, כך גם לגניבת אמצעי אחסון פיזיים

סעיף 18 : מדיניות ונהלי הגנה פיזית וסביבתית

תקנה 6 א'

יש לכתוב וליישם נהלים אשר יסייעו בהטמעת מדיניות הגנה פיזית וסביבתית והבקרות הרלוונטיות.

הסבר משלים : מטרת הבקרה הינה להנחות ולהגדיר את ראיית הארגון בנושאים כגון :

- נעילת ארגונים בסוף יום
- מצלמות אבטחה
- כניסת אורחים וכניסת עובדים חיצוניים למתחמי החברה ולאיזורים רגישים
- הגנה נאותה על חדרי השרתים וחדרי הבקרה וכו'

סעיף 19 : בקרת גישה פיזית

תקנה 6

יש לאכוף בקרת גישה פיזית בנקודות כניסה/יציאה למתקן

הסבר משלים : יש לתעד את הכניסות והיציאות של העובדים מאתרים בהם מצויות המערכות, וכן לתעד הכנסת ציוד אל מערכות המאגר והוצאת ציוד מהן. למשל באמצעות התקנת מצלמות, מערכת זיהוי ביומטרי וכו'.

סעיף 20 : בקרת גישה למכשירי פלט

תקנה 6

יש לשלוט בגישה פיזית למכשירי פלט של המערכת על מנת למנוע מגורמים בלתי מורשים להשיג את הפלט (לדוג' : מדפסות ופקסים)

הסבר משלים : מטרת הבקרה הינה לוודא כי המידע מגיע לבעליו המקורי. בקרה זו חשובה בפרט במקומות שבהם ישנו מידע פרטי כגון פקסים אשר כוללים מידע רפואי או ביטוחי, הדפסה של פרטים אישיים של עובדים וכו'.
במקרים אלו, חשוב לוודא כי המידע נחשף אך ורק למי שאמור להיחשף אליו.

סעיף 21 : ניהול כח אדם

תקנה 7 א'

יש לוודא כי ייקלטו לעבודה הקשורה למאגר המידע עובדים המתאימים לעבודה זו,
לאחר שננקטו אמצעים סבירים המקובלים בהליכי מיון עובדים ושיבוצם. יש לקחת בחשבון את רגישות המידע שבמאגר ואת היקף הרשאות הגישה לתפקיד שמיועד לו המועמד לתפקיד.

סעיף 22 : הדרכות ומודעות

תקנה 7 ב'

יש לקיים הדרכות לבעלי ההרשאות בנושא החובות לפי חוק הגנת הפרטיות והתקנות, בטרם יקבלו גישה למידע ממאגר המידע או לפני שינוי היקף הרשאותיהם.

הסבר משלים : יש לקיים פעילות הדרכה תקופתית אחת לשנתיים לפחות לבעלי ההרשאות

סעיף 23 : מדיניות ונהלים

תקנה 8 (א,ב)

יש לפתח, לתעד וליישם מדיניות בקרת גישה.

הסבר משלים : מדיניות בקרת הגישה נועדה לוודא כי רק גורמים מורשים יכולים לגשת למאגר מידע, לצפות ולבצע שינויים, וכל זאת בהתאם להגדרות תפקידם ובכפוף לפיקוח.

סעיף 24 : ניהול משתמשים

תקנה 8(א,ב), 9(ג)

יש לנטרל/להסיר חשבונות זמניים/לא פעילים באופן אוטומטי לאחר פרק זמן מוגדר ולבטל חשבונות של עובדים שעוזבים.

הסבר משלים : הארגון יגדיר תקופת זמן קבועה שלאחריה יחסמו חשבונות זמניים/לא פעילים באופן אוטומטי.

סעיף 25 : ניהול הרשאות

תקנה 8 א'

יש להגביל את הרשאות המשתמשים למינימום ההכרחי הדרוש לביצוע תפקידם

הסבר משלים: הארגון יגדיר רמת הרשאות מינימלית לכל תפקיד וכן רמת הרשאות מינימלית למשתמש בסיס (ללא תפקיד מוגדר) אך נדרשת לו גישה למאגר מידע.

הערות: ניתן לנהל את המשתמשים וההרשאות במערכת ניהול משתמשים אחת, אולם יש להגדיר רישום נפרד של ההרשאות לכל סביבה בנפרד.

סעיף 26: ניהול הרשאות

תקנה 8 א'

יש להגדיר בעלי תפקידים, לבצע הפרדה בין תחומי אחריות (Separation of duties) ולהביא אותה לידי ביטוי במתן הרשאות למאגר.

הסבר משלים: מטרת ההפרדה בין תחומי אחריות הינה להקטין את הפוטנציאל לשימוש לרעה של הרשאות.

הערות: ניתן לנהל את המשתמשים וההרשאות במערכת ניהול משתמשים אחת, אולם יש להגדיר רישום נפרד של ההרשאות לכל סביבה בנפרד.

סעיף 27: זיהוי ואימות

תקנה 9

אופן הזיהוי ייעשה ככל האפשר על בסיס אמצעי פיזי הנתון לשליטתו הבלעדית של המורשה.

הערות: בנוהל האבטחה יש לקבוע גם את:

- אופן הזיהוי. אם אופן הזיהוי מבוסס על סיסמאות - הנוהל יתייחס לחוזק הסיסמה, מספר הניסיונות השגויים, ותדירות החלפת הסיסמאות שתיעשה בהתאם לתפקיד מורשה הגישה, ובכל מקרה לתקופה שלא תעלה על 6 חודשים.
- ניתוק אוטומטי לאחר פרק זמן של אי-פעילות.
- אופן הטיפול בתקלות הקשורות באימות זהות.

סעיף 28: ניהול חיבורים (Sessions)

תקנה 9(ב)(2)

יש להגביל התחברות משתמש למערכת לאחר מספר ניסיונות התחברות כושלים, באמצעות נעילת האפשרות לביצוע התחברות במשך פרק זמן מוגדר או עד לשחרור ע"י מנהל מערכת.

הסבר משלים: מטרת הבקרה היא להתמודד עם הסיכון של התקפות מניעת שירות. יש ליישם את הבקרה בן ברמת החיבור למערכת ההפעלה והן ברמת חיבור לאפליקציות ספציפיות.

סעיף 29: ניהול חיבורים (Sessions)

תקנה 9(ב)(2)

יש לנעול חיבורים כתוצאה מחוסר פעילות זמני, ולא לאפשר את המשכיות החיבור עד להזדהות ואימות חוזר של המשתמש. כחלק מביצוע נעילת החיבור יש להסתיר מידע שהוצג על המסך טרם הנעילה.

הסבר משלים: בקרה זו מיושמת בדרך כלל ברמת מערכת ההפעלה, אך ניתן ליישמה גם ברמת האפליקציה. יש לציין כי נעילת חיבור אינה תחליף מקובל להתנתקות מהמערכת (Log-out).

סעיף 30 : הזדהות ואימות

תקנה 9(ב2)

יש לממש multifactor authentication לצורך התחברות מרחוק למאגר.

הסבר משלים: הארגון יישם הזדהות מרוחקת במספר אמצעי זיהוי (שניים או יותר) למערכות ארגון (מאגרי המידע הארגוויים).

סעיף 31 : הזדהות ואימות

תקנה 9 ג'

יש לנהל אמצעי הזדהות למערכת, לרבות: בחירת אמצעי זיהוי של עובד וחסימתם לאחר פרק זמן של חוסר שימוש.

הסבר משלים: יש לנהל מאגר של אמצעי הזדהות והנפקתם, כמו כן ניתן לבצע ביטול אמצעי הזדהות באמצעות מערכת מרכזית, ניתן לממש באמצעות מערכת לניהול הזדהות חזקה.

סעיף 32 : ניהול אירועים ודיווח

תקנה 10

יש לנהל מנגנון תיעוד אוטומטי (SOC) שיאפשר ביקורת על הגישה למערכות המאגר (מנגנון בקרה), אשר יכלול את הנתונים הבאים: זהות המשתמש, התאריך והשעה של ניסיון הגישה, רכיב המערכת שאליו בוצע ניסיון הגישה, סוג הגישה, היקפה, ואם הגישה אושרה או נדחתה.

הסבר משלים:

- ניהול אפקטיבי של אירועים וחשד לאירועים (התראות) רבים במקביל הינו תהליך מורכב.
- לטובת מעקב אחר סטטוס ההתראות, הפעולות הנדרשות לביצוע, מעקב אחר החלטות וכן נדרש למכן את החלקים שניתן בתהליך ניהול האירועים.

סעיף 33 : ניהול משתמשים

תקנה 10(א, ד)

יש לתעד ולנטר רישום אוטומטי (רישום Log) של כל יצירה, שינוי, אפשור, ניטרול והסרה של חשבון ושימוש חריג.

הסבר משלים: הארגון יתעד כל שינוי בחשבונות משתמשים וינהל מעקב אוטומטי או ידני ביצוע התיעוד. נתוני התיעוד של מנגנון הבקרה יישמרו למשך 24 חודשים לפחות.

סעיף 34 : תיעוד

תקנה 11 א'

נדרש לתעד אירועי אבטחה.

הסבר משלים: יש להתבסס על רישומים אוטומטים אודות אירועי אבטחה במערכות המאגר של הארגון, כגון syslog snmp.

סעיף 35 : ניהול אירועים ודיווח

תקנה 11 ב'

בנוהל האבטחה יש לקבוע הוראות לעניין התמודדות עם אירועי אבטחת מידע ואופן הדיווח לבעל המאגר

הערות : הארגון יישם מדיניות תגובה לאירועי אבטחת מידע כחלק ממדיניות אבט"מ הארגוני, הארגון יבדוק וירענן את התכנית אחת לתקופה.

סעיף 36 : ניהול אירועים ודיווח

תקנה 11 ב'

יש לפתח יכולת לטיפול באירועי סייבר ואבטחת מידע אשר כוללת הכנה, זיהוי וניתוח, בלימה והתאוששות.

הסבר משלים : מטרת הבקרה הינה להחזיק בידע והכלים הנדרשים מארגון לטובת תחקור אירוע, הכלתו, ניהולו בצורה יעילה והתמודדות עם ההשלכות שלו.

סעיף 37 : ניהול אירועים ודיווח

תקנה 11

יש לתעד אירועי אבטחת מידע, את תהליכי הטיפול באירוע לרבות איסוף מידע, פעולות שבוצעו ומסקנות.

הסבר משלים : הארגון ינהל דיווח מרוכז וכן ניהול אירועים מרוכז לטובת קבלת תמונה אחידה ומלאה לגבי אופי האירועי והערכת הסיכונים.

הערות : במאגר שחלה עליו רמת אבטחה בינונית - יתקיים דיון אחת לשנה לפחות באירועי האבטחה ויבחן את הצורך בעדכונו של נוהל האבטחה. במאגר שחלה עליו רמת האבטחה הגבוהה - ייערך דיון כאמור אחת לרבעון לפחות.

סעיף 38 : יישום הצפנה בהתקנים ניידים

תקנה 12

יש לממש מנגוני הצפנה על מדיה של התקנים ניידים (מחשבים ניידים, מכשירים סלולריים, טבלטים ועוד).

הסבר משלים : הארגון יממש הצפנה של דיסקים קשיחים של התקנים ניידים ושל התקני מדיה ניידים.

סעיף 39 : גישה באמצעות מכשירים ניידים

תקנה 12

יש ליישם מנגנוני הגנה לבקרת גישה לטלפונים ניידים, כגון שימוש בסיסמה או באמצעי ביומטרי

יש ליישם כלי הגנה ייעודיים המזהים וחוסמים גישה בלתי מורשית ויישומים עויינים על גבי מכשירים ניידים.

הסבר משלים :

- על הארגון להגדיר מדיניות שימוש בטלפונים ניידים לצרכי הארגון, לרבות גישה למאגרי מידע ושמירה של נתונים רגישים של הארגון על הטלפון.

- על הארגון לקבוע את הפרמטרים לבקרת גישה למכשירים ניידים כגון שימוש בסיסמה באורך מסוים ונעילה אוטומטית על מנת למנוע חדירת קוד עויין העלול לחשוף מידע רגיש/מאגרי מידע של הארגון, יש להפעיל יישומים ייעודיים המזהים ומונעים הפעלה של קוד עויין.

סעיף 40 : שימוש במדיה

תקנה 12

יש לכתוב וליישם מדיניות הגנה על מדיה (מגנטית, נתיקה, אופטית, מכנית), לבקר ולעדכן אותה באפן שוטף.

הסבר משלים : הארגון יכתוב ויישם מדיניות שימוש והגנה על מדיה הכוללת התייחסות לאופן שימוש במדיה, אחסון מדיה, ואופן השמדת המידע האגור במדיה ו\או השמדת המדיה עצמה בסוף השימוש (או סוף חיי המדיה)

סעיף 41 : הגנה על מידע בתנועה

תקנה 12

יש לממש מנגנוני הגנה על מנת למנוע דלף מידע בעת העברת מידע לגורמים פנימיים או חיצונים.

הסבר משלים : על הארגון ליישם מנגנונים להגנה על מידע בעת תנועה בין מערכות הארגון ובשליחתו אל גורמים מחוץ לארגון בהתאם למדיניות הגנת המידע הארגונית :

- מערכת למניעת דלף מידע
- מערכת להעברת מידע מאובטח כגון : מייל מאובטח/מוצפן, כספת

סעיף 42 : הגנת המידע השמור במשאבים משותפים

תקנה 12, 13 ב'

יש למנוע העברת מידע לא מורשית או לא מכוונת דרך משאבי מערכת משותפים.

הסבר משלים : על הארגון למנוע ולטפל בהעברת מידע לא מורשית באמצעות תיקיות משותפות, דואר אלקטרוני, מדיה נתיקה וכו' , ניתן ליישם באמצעות מערכת DLP.

סעיף 43 : ניהול מאובטח

תקנה 13 ב'

להפריד ככול האפשר בין מערכות המשמשות את מאגר המידע, כמו השרת שעליו מותקן המאגר, ותחנות הקצה בעלות גישה למאגר, משאר מערכות המחשבים הארגוניות שלא נדרש לגשת מהם למאגר המידע.
קיימות מספר שיטות להפרדה זו, למשל, מערכת FW פנימית

סעיף 44 : מדיניות ונהלים

תקנה 13 ג'

יש לכתוב וליישם מדיניות לניהול פגיעויות וחשיפות אבטחת מידע, וכן לבקר ולעדכן אותה תקופתית.

הסבר משלים:

- הארגון יגדיר מדיניות בנושא ניהול חשיפות בארגון הכולל: זיהוי פגיעויות וחשיפות והערכתן, תיקון החשיפות והפגיעויות, אחריות לביצוע המשימות ומעקב שוטף
- הארגון יכתוב תיק נהלים ותכנית ליישום ותפעול מערך ניהול הפגיעויות בדגש על הטמעת מערכות לזיהוי, הפעלת כלים וסוקרים, הפעלת ספקי משנה ועובדים לטיפול בממצאים.

סעיף 45: סריקות אבטחה

תקנה 13 ג'

יש לוודא כי כלי סריקת הפגיעויות מעודכן באופן שוטף ומכיל את הפגיעויות החדשות אשר מתגלות ומדווחות.

הסבר משלים:

יש לוודא שכלי הסריקה בעל יכולת עדכון שוטף, בעל רשיון בתוקף (על מנת לקבל עדכונים לגבי פגיעויות חדשות) וכן אכן מתבצע עדכון של הפגיעויות שהכלי מסוגל לזהות.

הערות: נדרש לעדכן באופן שוטף את מערכות המאגר, חומרה ותוכנה בהתאם להנחיות היצרן על מנת לנטרל פגיעויות וחולשות המתגלות מעת לעת.
לא יעשה שימוש במערכות (חומרה או תוכנה) שהיצרן שלהן הפסיק את התמיכה בהיבטי האבטחה שלהן.

סעיף 46: יישום הצפנה

תקנה 14(א,ב)

יש לממש מנגנוני הצפנה למידע רגיש המועבר בין מערכות לבין ממשקי משתמש קצה למידע רגיש המועבר בין מערכות בתוך הארגון ומחוץ לארגון.

הסבר משלים: הארגון יגדיר ויממש מערכי הצפנת נתונים למידע רגיש המוצג למשתמש באמצעות דפדפן, אפליקציית מובייל או מערכות אחרות המנגישות מידע באמצעות רשתות ציבוריות כגון רשת האינטרנט או בתוך הארגון.

דוגמא: שימוש בתעודות SSL מאושרות ועדכניות בדפדפן, הארגון יממש תעבורה מוצפנת בממשקים בין שרתים ושירותים המעבירים מידע רגיש וכן יעדיף שימוש בפרוטוקולים המצפינים תעבורה.
שימוש בפרוקולים כגון SSL,SSH,HTTPS,SFTP.

סעיף 47: גישה מרחוק

תקנה 14 ב'

יש לממש מנגנונים להצפנת התווך לצורך הגנה על סודיות ושלמות התחברויות מרחוק.

הסבר משלים: גישה מרחוק למערכות מידע ארגוניות מוגדרת כביצוע חיבור ע"י משתמשים או תהליכי מחשב מתוך רשתות חיצוניות.

הערות: ארגונים נוהגים להטמיע רשתות וירטואליות מוצפנות (VPN) על מנת להגביר את סודיות ושלמות החיבור. לדוגמא: שימוש ב OWA ללא OTP.

סעיף 48 : גישה מרחוק

תקנה 14 ג'

יש לנטר התחברויות מרחוק.

הסבר משלים : ניטור אוטומטי של חיבורים מרחוק מאפשר לארגונים לזהות התקפות סייבר, ובנוסף מאפשר לוודא ציות לנהלי הגישה מרחוק באמצעות בקרה על פעילויות המתבצעות במהלך החיבור המרוחק.

סעיף 49 : הזדהות ואימות

תקנה 14 ג'

יש ליישם כלי הגנה ייעודיים המזהים וחוסמים גישה בלתי מורשית ויישומים עויינים על גבי מכשירים ניידים.

הסבר משלים : הארגון יאמת באופן חד ערכי משתמש המתחבר למערכות הארגון.

הערות : במאגרים ברמת האבטחה הבינונית והגבוהה יש לעשות שימוש באמצעי פיזי, הנתון לשליטתו הבלעדית של בעל ההרשאה, כגון כרטיס חכם.

סעיף 50 : אמצעי הגנה

תקנה 14 א'

התקנת אמצעי הגנה מפני חדירה לא מורשית, או תוכנות מזיקות. כגון : תוכנת אנטי-וירוס, תוכנת Fire Wall. את אמצעי ההגנה יש ליישם הן בממשק של מערכות המאגר לרשת האינטרנט או הרשת החיצונית, הן בממשקים בין המערכות ככול שקיימים והן בממשק בין מערכות הקצה הניגשות למערכות המאגר.

סעיף 51 : מדיניות אבטחת שרשרת האספקה

תקנה 15

הארגון יכתוב מדיניות ונוהל לתהליכי ניהול שרשרת האספקה המשלבת חשיפה לנכסים שהוגדרו.

הסבר משלים : הארגון יכתוב מדיניות סדורה אשר תופץ לכל בעלי התפקידים בתהליכי רכש וניהול חוזים. תהליך העבודה מחויב לשלב את כלל הבקרות הנדרשות בכדי לודא כי תהליכי הרכב מתבצעים בתצורה מאובטחת.

הערות : יש לפרט בנוהל האבטחה של המאגר גם את העניינים שפורטים בתקנה 15.

סעיף 52 : יישום תקנות הגנת הפרטיות עבור התקשרות עם מיקור חוץ המשלב מידע מתוך מאגר או מאגר שלם

תקנה 15

ממונה אבטחת המידע לתחום הגנת הפרטיות יוודא יישום תקנה 15 במסגרת הליך ההתקשרות והעברת המידע למיקור חוץ.

הסבר משלים : ניתן לממש ע"י האמצעים הבאים :

1. הארגון יבחן, לפני ביצוע ההתקשרות עם הגורם החיצוני המסוים כאמור, סיכוני אבטחת המידע הכרוכים בהתקשרות.

2. הארגון יקבע במפורש בהסכם עם הגורם החיצוני :

- מהו המידע שהגורם החיצוני רשאי לעבד ולאלו מטרות?
- לאלו מערכות הוא רשאי לגשת?
- מהו סוג העיבוד שאותו הוא רשאי לבצע?
- מהו משך ההתקשרות ומה יהיה אופן השבת המידע לידי הבעלים בסיום ההתקשרות?
- אופן יישום הוראות תקנות אבטחת מידע.
- חובתו של הגורם החיצוני להחתים את בעלי ההרשאות שלו על התחייבות לשמור על סודיות המידע
- אם בעל המאגר התיר לגורם החיצוני לתת את השירות באמצעות גורם נוסף - חובתו של הגורם החיצוני לכלול בהסכם עם הגורם הנוסף את כל הנושאים המפורטים בתקנה זו (תקנה 15)
- חובתו של הגורם החיצוני לדווח, אחת לשנה לפחות, לבעל מאגר המידע על אודות אופן ביצוע חובותיו לפי תקנות אלה וההסכם, ולהודיע לבעל המאגר במקרה של אירוע אבטחה.

3. הארגון יפרט בנוהל המאגר את דבר ההתקשרות והתהליכים הרלוונטיים.
4. הארגון ינקוט אמצעי בקרה עפ"י הסיכונים שהוגדרו ובהתאמה להסכם הרשום.

<u>סעיף 54 : דרישות אבטחה מספקי מערכות ושירותים</u>

<u>תקנה 15 א'</u>

יש להתגונן מפני איומים של שרשרת האספקה על המערכת כחלק מאסטרטגיית "הגנה לעומק" (Defense in Depth).

<u>הסבר משלים</u> : הארגון ימפה ויזהה את האיומים והסיכונים הנובעים משימוש במערכת / שירות הספק על האספקטים הטכנולוגיים והתהליכיים הגלומים בהם, ויגלם את הסיכונים כחלק מתהליך ניהול הסיכונים והאיומים הארגוני.

<u>סעיף 55 : דרישות אבטחה מספקי מערכות ושירותים</u>

<u>תקנה 15 א'</u>

במקרים בהם יש חיבור לרשת הספק, יש ליישם בקרות מונעות אשר תפקידן למזער נזק המגיע מתשתיות הספק.

<u>הסבר משלים</u> : הארגון ישתמש בבקרות הקיימות אצלו או בקרות יעודיות אחרות על מנת למזער את הנזק ממערכות / שירותי הספק.

<u>סעיף 56 : בדיקות ציות טכניות</u>

<u>תקנה 16 א'</u>

יש לוודא כי מערכות המידע השונות עומדות בסטנדרט אבטחת המידע/הגנת סייבר הארגוני וכי הן מיושמות באופן מאובטח על בסיס קבוע - בהתאם למדיניות אבטחת המידע והגנת הסייבר הארגונית ונוהל האבטחה.

הסבר משלים: אחת ל-24 חודשים לפחות יש לערוך ביקורת פנימית או חיצונית, על ידי גורם בעל הכשרה מתאימה לביקורת בנושא אבטחת מידע, שאינו ממונה האבטחה של המאגר, על מנת לוודא עמידתו בהוראות התקנות.

סעיף 57: תכנית המשכיות עסקית

תקנה 17,18

יש לכתוב וליישם מדיניות המשכיות עסקית, בהיבטי הגנת סייבר, לבקר ולעדכן אותה תקופתית.

הסבר משלים:

- הארגון יכתוב ויישם תכנית המשכיות עסקית אשר נגזרת מיעדי הארגון ומיישמת בקרות ותהליכים על מנת לעמוד ביעדים אשר הוגדרו.
- התוכנית תתחשב בתרחישי האסון השונים ובתהליכים הקריטיים למימוש יעדי הארגון.

במאגר שחלה עליו רמת האבטחה הגבוהה חלה דרישה נוספת - בעל המאגר אחראי לכך שיישמר עותק הגיבוי של הנתונים הנ"ל באופן שיבטיח את שלמות המידע ואת אפשרות השחזור של המידע במקרה של אובדן או הרס. למשל שמירת הגיבוי באתר פיזי אחר.

הערות: יש לקבוע במסמך את הנהלים הבאים:

- נהלים לביצוע גיבוי נתוני אבטחה באופן תקופתי שגרתי.
- נהלים שיבטיחו שניתן יהיה לשחזר את הנתונים באופן יעיל ומהיר, ובלבד שביצוע השחזור יהיה באישור מנהל המאגר.
- במסגרת תיעוד אירועי אבטחה, יתועדו גם הליכי שחזור המידע, ובכלל זה - זהותו של מי שביצע את הליכי השחזור ופרטי המידע ששוחזר.

תקנה: 17 א'

יש לשמור את הנתונים "הטכניים" הנצברים במסגרת יישום התקנות, באופן מאובטח למשך 24 חודשים (נתוני בקרה על כניסה ויציאה מאתרי המערכות, הכנסה והוצאה של ציוד אל מערכות המאגר ומהן, ניהול הרשאות גישה, זיהוי ואימות, בקרהותיעוד גישה, תיעוד של אירועי אבטחה, אבטחת תקשורת, אמצעי בקרה ופיקוח על הגורם החיצוני בעל גישה למאגר וביקורות תקופתיות)

הערות: יש לגבות את הנתונים שנשמרו, באופן שיבטיח שיהיה ניתן, בכל עת, לשחזר את הנתונים האמורים למצבם המקורי