מדיניות אבטחת המידע

גירסא 1.1

מעקב גרסאות

מס"ד	תאריך	עודכן על ידי	תיאור השינויים
1.0	18-5-2015	אופיר יהב	גרסא ראשונה לאחר הסבה מתבנית ישנה – נוהל 5.1 בפרק אחריות הנהלה – לתבנית מסמך ממשל זמין חדש. עדכון לאחר מעבר ממשרד האוצר למשרד ראש הממשלה עדכון שם מערך הסייבר ואבטחת המידע.
1.1	8.2.2016	אופיר יהב	הוספת נספח מערכות קריטיות – הנדרש על פי תקן ISO-27001

נתוני גרסת המסמך

גורם	תפקיד	שם מלא	תאריך	חתימה
נערכה ע"י	PMO	אופיר יהב	8.2.2016	(חתימה)
נבדקה ע"י	מוביל טכנולוגיות במערך סייבר ואבט"מ	אלעד פז	8.2.2016	(חתימה)
אושרה ע"י	מנהל מערך סייבר ואבטחת המידע	אברהם זרוק	8.2.2016	(חתימה)

תוכן עניינים

1. כללי

- ממשל זמין מחויב לדרישות והנחיות תקן ISO-27001-2013 ובמסגרת פרק הנהלה יש לפרט את מדיניות אבטחת המידע.
- מסמך זה מחליף את מסמך A.5.1 – מדיניות אבטחת המידע – בתבנית הישנה.

2.רקע:

2.1. מדיניות אבטחת המידע בממשל זמין, מהווה את הבסיס הארגוני להחלטות ההנהלה, לפיו יש לתת מענה ארגוני, אמצעים ומשאבים כלכליים, תוך מיסוד נכון של תהליכי קבלת החלטות ניהול ובקרה במסגרת אחריות מוגדרת.

2.2. פעילותו התקינה של ממשל זמין מושפעת ותלויה ברמת שלמות המידע, סודיותו, אמינותו, עדכניותו, זמינותו ושרידותו.

3.מטרה:

3.1. להתוות את מדיניות אבטחת המידע בממשל זמין שנועדה לצמצם פגיעה במידע, במאגריו ובמערכותיו ומתוך כך יצומצמו סיכוני הפגיעה בתפעולו הסדיר של ממשל זמין וכתוצאה מכך גם במקבלי השירות של ממשל זמין.

4.אחריות:

4.1. ועדת ההיגוי לאבטחת מידע אחראית לגיבוש ולעדכון המדיניות בתחום, להתוות אסטרטגיות פעילות, לפקח אחר תוכניות העבודה השנתיות, לקיים הערכת נזקים בעקבות תקלות ולגבש המלצות לטיפול.

4.2. אחראי הסמכות ורגולציה בממשל זמין, אחראי לעדכון המדיניות עפ"י החלטות וסיכומי ועדת היגוי לאבטחת המידע.

5.הגדרות:

5.1. **מידע**: כל נתון הנוגע ו/או הקשור לפעילותו, תפעולו או תפקודו של ממשל זמין, לרבות מידע הנוגע לצנעת הפרט ומידע ממשלתי רגיש, הקיים על-גבי אמצעי אחסון ממוחשבים, מגנטיים או אלקטרונים, על-גבי מצעי מידע פיזיים וכן המועבר בעל-פה.

5.2. **אבטחת מידע**: מכלול הפעולות והאמצעים הננקטים והמיושמים בממשל זמין, שמטרתם להביא לכך שהמידע ופריטי הציוד היוצרים אותו ומטפלים בו, יוגנו מפני פגיעה, חשיפה או שינוי, במזיד או בשוגג, הן מתוככי מסגרת ממשל זמין והן מחוצה לו.

5.3. **ועדת היגוי לאבטחת מידע**: ועדה הכוללת נציגים מממשל זמין אשר נועדה לגבש ולעדכן את מדיניות ממשל זמין בתחום אבטחת המידע, להתוות אסטרטגיות פעילות, לפקח אחר תוכניות העבודה השנתיות, לקיים הערכת נזקים בעקבות תקלות ולגבש המלצות לטיפול.

5.4. **מנהל מערך הסייבר ואבטחת מידע**: מנהל מערך הסייבר ואבטחת המידע בממשל זמין, אשר מנחה ונותן תמיכה בתחום אבטחת המידע בממשל זמין ואשר מנחיל את החלטות וסיכומי ועדת היגוי לאבטחת המידע.

5.5. **אחראי הסמכות ורגולציה**: גורם בממשל זמין שמונה לתפקיד ע"י מנהל ממשל זמין והמסייע בידו לקיים את פעילות אבטחת המידע והאיכות השוטפת, כמוגדר על-ידי מנהל מערך הסייבר ואבטחת המידע ומנהלי פרויקטים שונים, כנגזר משיטות, תהליכי וכלי העבודה המיושמים.

5.6. **בעל המידע**: מנהל (עובד משרד ממשלתי) אשר הוגדר שכזה על-ידי ממשל זמין ואשר הינו המשתמש העיקרי במידע בתחום מסוים, או שהמידע נוצר בתחום אחריותו. בעל המידע יסייע בהגדרת סודיות, רגישות וחיוניות המידע וימליץ בפני מנהל מערך הסייבר ואבטחת המידע על סיווגו של המידע ועל הטיפול הנגזר מתוקף כך.

5.7. **מנהל מאגר**: גורם אשר הוסמך מטעם המשרד הממשלתי בו הינו מועסק, לנהל מאגר מידע מסוים ואשר נרשם במשרד המשפטים כמנהלו של המאגר.

5.8. **אורח**: גורם שאינו נמנה על עובדי ממשל זמין, אשר קיבל היתר מוגבל בזמנים לשהות במתחם העבודה, או לעשות שימוש במערכות המחשב של ממשל זמין ולהיחשף, או לעשות שימוש במידע בכפוף לנוהלי ממשל זמין.

5.9. **שימוש אסור**: פעולה המבוצעת מבלי לקבל היתר לביצועה על-פי נהלי ממשל זמין וכן פעולה שהותרה לביצוע, אך אינה "כשרה" בנסיבות ביצועה.

6.מסמכים ישימים

6.1. תקן ת"י ISO 27001 – פרק A.5.1

7.עיקרי מדיניות אבטחת המידע:

7.1. כללי

הנהלת ממשל זמין מחויבת לתחום אבטחת המידע באופן הכולל קביעת מטרות, תוכניות עבודה, תפקידים ואחריות בנושאי אבטחת מידע, הפצת מדיניות אבטחת המידע בממשל זמין, אספקת משאבים להקמה וניהול מערך אבטחת מידע, קביעת סיכונים ורמות סיכונים, ביצוע סקרי אבטחת מידע, סקרי הנהלה ומבדקים פנימיים וביצוע הדרכות אבטחת מידע לעובדי ממשל זמין ולעובדים האחראים על תפעול מערך אבטחת המידע של ממשל זמין.

7.2. ממשל זמין נסמך על מדיניות ונהלי אבטחת המידע של משרד ראש הממשלה וכפוף לאגף חירום ובטחון של משרד ראש הממשלה בנושאי אבטחת מידע אשר בתורו מונחה על ידי הרשות לבטחון המידע בשרות הבטחון הכללי. בשל ייחודו של ממשל זמין, ישנו צורך במסמך מדיניות אבטחת מידע ונהלים נפרדים וייחודיים, אשר יכסו את פעילותו של ממשל זמין.

7.3. מבנה ממשל זמין:

7.3.1. הנהלה

7.3.2. מערך סייבר ואבטחת המידע

7.3.3. מטה וניהול לקוחות

7.3.4. טכנולוגיות

7.3.5. מוצרים ויישומים

7.3.6. פיתוח

7.3.7. זהות דיגיטלית

7.4. אבטחת מידע כוללת את התחומים הבאים:

7.4.1. אבטחה פיזית.

7.4.2. אבטחת רשומות.

7.4.3. אבטחה לוגית.

7.4.4. מהימנות עובדים.

7.4.5. אבטחת ממשקים עסקיים.

7.5. אבטחת המידע בממשל זמין תיושם בכפוף ובצמידות לחוקים, לתקנות והנחיות הנוגעים לתחום אבטחת מידע, לרבות חוק המחשבים וחוק הגנת הפרטיות ותקנותיו ובהתייחס להחלטות ועדת היגוי לאבטחת מידע. מערך אבטחת מידע יתאים לדרישות התקן ת"י ISO 27001 בהקשר של שיפור מתמיד, כך שיענה לדרישות מודל ה-PDCA של תקן ת"י ISO 9001:2008.

7.6. מבנה ארגוני/פונקציונלי ליישום ולניהול אבטחת המידע:

7.6.1. ועדת היגוי לאבטחת מידע - ועדה הכוללת נציגים מתתי פרויקטים שונים של ממשל זמין, אשר נועדה לגבש ולעדכן את מדיניות ממשל זמין בתחום אבטחת המידע, להתוות אסטרטגיות פעילות, לפקח אחר תוכניות העבודה השנתיות, לקיים הערכת נזקים בעקבות תקלות ולגבש המלצות לטיפול.

7.6.2. בעלי תפקידים בוועדה:

7.6.2.1. מנהל/סגן מנהל ממשל זמין– יו"ר הועדה.

7.6.2.2. מנהל מערך הסייבר ואבטחת המידע – מזכיר הועדה.

7.6.2.3. נציגי ההנהלה

7.6.2.4. מנהלי תתי פרויקטים רלוונטיים (פירוט בנוהל "1.4 – תפקידים ואחריות").

7.6.3. **מנהל מערך הסייבר ואבטחת מידע**: תמיכה שוטפת בתחום אבטחת המידע בממשל זמין והנחלה בשטח של החלטות וסיכומי ועדת היגוי לאבטחת המידע.

7.6.4. **אחראי הסמכות ורגולציה**: קיום ויישום של תהליכי, שיטות וכלי אבטחת המידע, ביחידות מרוחקות, כמוגדר על-ידי מנהל מערך הסייבר ואבטחת מידע.

7.7. סיווג מידע:

7.7.1. במסגרת ועדת ההיגוי יגובשו קריטריונים להגדרת סיווג רגישות המידע וחיוניותו, לפי מידת הנזק שייגרם לממשל זמין, למדינת ישראל ו/או לגורמים אחרים, כתוצאה מחשיפה, חבלה או שיבוש של המידע, מאגריו או מערכותיו, בין אם במזיד ובין אם בשוגג.

7.7.2. סיווג המידע יתייחס לכל מצע, או מאגר בהם קיים המידע (קבצים, בסיסי נתונים, מצעי מדיה אלקטרונית, או אופטית, מסמכים, דו"חות וכדומה).

7.7.3. סיווגו של המידע יקבע בהתאם לרמת הרגישות הגבוהה ביותר הקיימת בקובץ, במאגר או במצע הפיזי בהם אגור המידע (על-פי עקרון "המחמיר קובע").

7.7.4. מנהל מערך הסייבר ואבטחת המידע יקבע את רמת האבטחה הנדרשת לכל סיווג ויסווג את משאבי המידע בהתאם.

7.8. רמת אבטחת מידע מחייבת:

7.8.1. באחריות מנהל מערך הסייבר ואבטחת המידע לקבוע את רמת האבטחה המחייבת את יוצרי המידע, מאגריו ומערכותיו.

7.8.2. רמת האבטחה תקיף ותכסה את המידע על כל התחומים הנגזרים ממנו (אבטחה פיזית, אבטחת רשומות, אבטחה לוגית, אבטחת מהימנות עובדים ואבטחת ממשקים עסקיים).

7.8.3. רמת האבטחה בכל מערכת מידע, לא תהיה פחותה מרמת האבטחה של המידע ברמת הסיווג הגבוהה ביותר, המנוהל על ידי מערכת המידע.

7.8.4. רמת אבטחת המידע בכל המערכות ומתקני ממשל זמין, לא תהיה פחותה מרמת האבטחה המחייבת הנמוכה ביותר שתקבע.

7.8.5. כל דרישה לחריגה מרמה זו תובא מנומקת לאישור מראש של מנהל מערך הסייבר ואבטחת המידע.

7.9. אבטחה פיזית:

7.9.1. מדיניות האבטחה בממשל זמין, כוללת ממספר מעגלי אבטחה, אשר במרכזם ניצבים נכסיו היקרים של ממשל זמין, אותם הוגדר שיש צורך לאבטח, בדגש על מידע המהווה את הנכס העיקרי והמהותי ביותר בממשל זמין.

7.9.2. מעגל האבטחה החיצוני כולל את היבטי האבטחה הפיזיים אשר נותנים מענה ראשון למתקפות כנגד ממשל זמין (במכוון או בשוגג), באשר הן.

7.9.3. רגישותן הגבוהה של המערכות הממוחשבות וחשיבותו של המידע האגור בהן, מחייבים מידור פיזי של המורשים בגישה למערכות אלו. אמנם קיימים מעגלי אבטחה נוספים (לוגיים, בין היתר) אשר נועדו למנוע נגישות בלתי מורשית למידע, אך אין להתבסס עליהם בלבד ויש למנוע נזקים פוטנציאליים עוד באיבם, תוך איתורם באפיקים הפיזיים, כבר בכניסות לבניין, ב"איזורים הסטריליים" וכו' (טרם הגעה למערכות הממוחשבות עצמן).

7.9.4. מנהל מערך הסייבר ואבטחת המידע יגדיר הרשאות גישה לרכיבי המערכת השונים, לרבות מחשבים וציוד תקשורת וכן את דרכי האכיפה והבקרה על ביצוען.

7.9.5. מנהל הביטחון בהנחיית גורמי ההנחייה השונים, יקבע רמת אבטחה פיזית מחייבת. ובכלל זה יקבע:

7.9.5.1. דרישות מבנה ותנאים סביבתיים.

7.9.5.2. שיטות וכלים למידורי כניסה.

7.9.5.3. תהליכים ואמצעי בקרה (לדוגמא: טמ"סים, מאבטחים, תגי כניסה).

7.9.5.4. טיפול בחריגים.

7.9.5.5. אופן ביצוע פיקוח ובקרה.

7.10. אבטחת רשומות:

7.10.1. רשומות מידע כוללות מצעי מידע פיזיים כגון מסמכים, תדפיסים, דיסקים, קלטות וסרטים.

7.10.2. אבטחת רשומות חיונית משום קיומו של מידע רגיש רב על-גבי מצעים פיזיים אשר הגעתם לידיים עוינות עלולה להוביל לנזקים. בנוסף לסיכוני אבטחת המידע הקיימים לרשומות הנמצאות בשטח העבודה בממשל זמין, מידע ברשומות עשוי לעתים להימצא מחוץ לשטח ממשל זמין (לצרכי ישיבות או עבודה מרחוק וכן משום השלכת מסמכים לפחי אשפה הנלקחים מחוץ לבניין), שם הנו חשוף לסיכונים נוספים.

7.10.3. מנהל מערך הסייבר ואבטחת המידע יגדיר את אמצעי ותהליכי הטיפול באבטחת רשומות, בהתאם לרגישות המידע. תחומי ההתייחסות יכללו:

7.10.3.1. שיטות וכלים לאבטחת מידע והשמדתו, בהתאם לסיווג המידע.

7.10.3.2. תהליכי ואמצעי שינוע מידע (פנים וחוץ ארגוני).

7.10.3.3. טיפול בחריגים.

7.10.3.4. אופן ביצוע פיקוח ובקרה.

7.11. אבטחה לוגית:

7.11.1. האבטחה הלוגית מהווה את ה"שכבה" העיקרית והקרובה ביותר בהגנה על המידע המצוי במערכות המחשב והתקשורת.

7.11.2. העדר יישום נכון של "שכבה" זו, חושף את המידע לפעילויות שונות, אשר חלקן עלולות להסב נזק רב לממשל זמין.

7.11.3. מנהל מערך הסייבר ואבטחת המידע יתווה את רמת האבטחה הלוגית המחייבת עבור רכיביהן השונים של מערכות המחשוב והתקשורת.

7.11.4. תיושם הגנה לוגית במערכות ההפעלה, בתוכנות ובאפליקציות, בקבצי ובבסיסי נתונים, בפעולות שינוי של הנתונים (ברמת הרשומה, השדות וסוג הפעולה) ובתקשורת.

7.11.5. תחומי התייחסות של מנהל מערך הסייבר ואבטחת המידע בהיבטים הלוגיים יכללו התוויה, הגדרה ובקרת יישום של:

7.11.5.1. שיטות וכלים לאבטחת מידע במערכות המחשב והתקשורת, בהתאם לסביבות העבודה ולהגדרות הפרופילים שיקבעו.

7.11.5.2. טיפול בחריגים.

7.11.5.3. אופן ביצוע פיקוח ובקרה.

7.12. איסור שינוי לא מבוקר:

7.12.1. יוגדרו נהלים המתווים את אופן ביצוע השינויים בנתונים, בתוכנות יישומיות, בתוכנות תשתית ובחומרה, של מערכות ממשל זמין.

7.12.2. חל איסור על ביצוע שינוי בנתונים שלא במהלך הפעילות הרגילה, בתוכנה יישומית, בתוכנת תשתית ובחומרה, אלא אם הדבר נעשה באופן מאובטח ומבוקר ובהתאם להנחיות מנהל מערך הסייבר ואבטחת המידע, תוך התייעצות עם גורמי ההנהלה הרלוונטיים.

7.12.3. מנהל פרויקט רלוונטי יוכל לבצע שינויים בפרויקט עליו הוא אחראי, בהתאם לצורך, ובתנאי שהתייעץ בנושא עם מנהל מערך הסייבר ואבטחת המידע וקיבל את אישורו המוקדם לכך.

7.13. מידור המידע והרשאות גישה:

7.13.1. יבוצע מידור של המידע ושל המשתמשים בו. לכל פרופיל משתמש יוענקו הרשאות גישה לפרטי מידע הדרושים לו לביצוע עבודתו בלבד, כפי שיוגדר על ידי מנהל מערך הסייבר ואבטחת המידע בשיתוף בעלי המידע, בהתאם לעקרון "הצורך לדעת".

7.13.2. מידור המידע יעשה על ידי חלוקת המידע והמשתמשים לקבוצות שייכות או עניין ובהתאם לסביבות העבודה (פרופילי משתמשים).

7.13.3. עקרונות המידור יוגדרו על-ידי מנהל מערך הסייבר ואבטחת המידע והגורמים המקצועיים בכל תחום פעילות בממשל זמין.

7.14. מהימנות עובדים:

7.14.1. מהימנות העובדים ויושרם הנם בסיס לאבטחת מידע, מעצם חשיפתם למידע ומתוקף היותם המפעילים, המאפיינים, המתחזקים והמשתמשים במערכות המידע, מאגריו ומצעיו.

7.14.2. על הנהלת ממשל זמין ועל המנהלים השונים הקולטים עובדים חדשים לוודא יישום הליכי בקרה הנוגעים ליושרם ולאמינותם של העובדים החדשים הנקלטים בממשל זמין.

7.14.3. אגף חרום וביטחון במשרד ראש הממשלה, יגדיר להנהלת ממשל זמין את הסיווגים הביטחוניים הנדרשים מעובדי ממשל זמין, תוך התייחסות לקריטריונים ספציפיים הנוגעים לרגישות המידע אליו יחשפו.

7.14.4. אגף חרום וביטחון במשרד ראש הממשלה יתווה ויגדיר את יישומם של:

7.14.4.1. תהליכים ואמצעים לווידוא מהימנות עובדים, בהתאם לצורך.

7.14.4.2. טיפול בחריגים.

7.14.4.3. אופן ביצוע פיקוח ובקרה.

7.15. אבטחת ממשקים עסקיים:

7.15.1. בממשל זמין משולבים ממשקים עסקיים רבים, המספקים שירותי חוץ בתחומי פעילות שונים.

7.15.2. הממשקים העסקיים נבדלים זה מזה בהיקף ואופן חשיפתם למידע המצוי בממשל זמין. חלקם רשאים להיכנס לאזורי עבודה מסוימים אך אמורים להיות מנועים מחשיפה למידע רגיש (כגון עובדי ניקיון), בעוד לאחרים הרשאות גישה גורפות לכלל מערכות המידע, הנתונים ואזורי העבודה.

7.15.3. יחד עם עובדת היתר עבודתם של ממשקים חיצוניים בשטח העבודה, קיימים ממשקים עסקיים המורשים לעבוד מחוץ למשרדי ממשל זמין.

7.15.4. נסיבות עבודה אלו, מהוות סיכון אבטחתי גדול העלול להוביל לתרחישי דלף מידע.

7.15.5. מנהל מערך הסייבר ואבטחת המידע יתווה תהליכי ושיטות טיפול אבטחתי בממשקים עסקיים, לרבות:

7.15.5.1. קריטריונים להגדרת רגישות/סיווג הממשק העסקי.

7.15.5.2. דרישות אבטחתיות בכפוף לסיווג הממשק העסקי.

7.15.5.3. שיטות וכלים לאכיפת הדרישות.

7.15.5.4. תהליכים ואמצעים לפיקוח ובקרה ולטיפול בחריגים.

7.16. אחריות אישית לאבטחת מידע:

7.16.1. כל עובד אחראי באופן אישי לכלל המידע המצוי בחזקתו, לרבות כזה אשר נשלח או הועבר אליו על-ידי גורם אחר.

7.16.2. כל עובד אחראי באופן אישי לאבטחת המידע בנושאים עליהם הוא מופקד.

7.16.3. מנהלים ישאו באחריות כוללת ליישום נהלי אבטחת המידע בתחומי סמכותם, לפעילות הולמת של עובדיהם מהיבטי האבטחה וכן לטיפול בנושאי אבטחת מידע חריגים בשיתוף עם מנהל מערך הסייבר ואבטחת מידע.

7.16.4. האחריות לאבטחת המידע, בין אם הנה מוטלת על עובדי ממשל זמין ובין אם על מנהליו, מתייחסת לאבטחה הפיזית, אבטחת הרשומות והאבטחה הלוגית.

7.16.5. הנהלת ממשל זמין מצפה מכל עובד לראות עצמו כאחראי ולפעול לדווח ישירות ומיידי למנהל מערך הסייבר ואבטחת המידע, על כל פעילות העלולה להשפיע על אבטחת המידע.

7.17. שינויים טכנולוגיים:

7.17.1. כל שינוי במפרטים הטכניים של המערכות, שעשוי לשנות את מצב אבטחת המידע, מחייב מעורבות של מנהל מערך הסייבר ואבטחת המידע.

7.17.2. בכל מקרה של חוסר וודאות לגבי הצורך במעורבותו של מנהל מערך הסייבר ואבטחת המידע, יש לפנות למנהל מערך הסייבר ואבטחת המידע טרם ביצוע השינוי.

7.18. אבטחת מידע בתהליך הפיתוח והתחזוקה:

7.18.1. מנהלי הפרויקטים יידעו את מנהל מערך הסייבר ואבטחת המידע על כל כוונה לבצע שינוי מהותי במערכות המידע בממשל זמין, ברמת חומרה, או תוכנה.

7.18.2. מנהל מערך הסייבר ואבטחת המידע אחראי להגדרת דרישות אבטחת מידע, במידת הצורך, בנושאים שבפיתוח ובתחזוקה.

7.19. בקרה וכלי בקרה:

7.19.1. מנהל מערך הסייבר ואבטחת המידע יגדיר ויתווה את אמצעי ותהליכי הבקרה בתחומי אבטחת המידע של ממשל זמין.

7.19.2. באחריות מנהל מערך הסייבר ואבטחת המידע לבקר, בצורה שוטפת ו/או אקראית, את הפעילויות המתבצעות על/עם המידע, בכדי לוודא כי ממשל זמין עומד בדרישות החוקים, התקנות, התקנים והנהלים ובהתאם לכללי המנהל התקין.

7.19.3. בידי מנהל מערך הסייבר ואבטחת המידע יינתנו כלים זמינים לבקרת פעילויות אבטחת המידע השוטף בגופים ובאתרים השונים של ממשל זמין.

7.19.4. הבקרה על יישום מדיניות ונהלי אבטחת המידע עפ"י ת"י ISO27001 תנוהל ע"י מערכת ממוחשבת ייעודית. ניהול המערכת יבוצע ע"י אחראי הסמכות ורגולציה בממשל זמין, בשיתוף מנהלי מחלקות בממשל זמין.

7.20. נתיב ביקורת

7.20.1. יישמו כלים המאפשרים זיהוי חד-ערכי של משתמשים אשר ביצעו שינויים במידע או בתוכנה, או אשר ניגשו למידע רגיש, תוך פירוט הפעילות שבוצעה וזמן הביצוע, לפי הגדרות מנהל מערך הסייבר ואבטחת מידע.

7.20.2. כלים אלה יעבדו וינהלו רישום הפעילות בשתי רמות:

7.20.2.1. כלי לזיהוי ולרישום גישה לרשת מגורמים מרוחקים, ניסיונות חדירה וגישה לקבצים רגישים. כלי זה יעקוב אחר הפעילות ברמת הרשת.

7.20.2.2. תיעוד ברמת האפליקציה של גישה למידע רגיש על-ידי משתמש. התיעוד יבדיל בין שינוי נתונים לקריאתם.

7.21. טיפול באירועי אבטחת מידע חריגים:

7.21.1. לכל פעילות חריגה בעלת השלכות על אבטחת המידע יוגדר אופן רישומה, הדיווח עליה ואופן התגובה הנדרש.

7.21.2. חריגות בתחום אבטחת המידע המאותרות על-ידי גורמי ממשל זמין, או אחרים, ידווחו למערך הסייבר ואבטחת המידע או המנהל הרלוונטי.

7.21.3. הנהלת ממשל זמין תגיב על אירועי אבטחת מידע חריגים.

7.21.4. במקרים של אירועי אבטחת מידע חריגים, יועבר דיווח לוועדת היגוי לאבטחת המידע.

7.22. תכנית היערכות להמשכיות עסקית (DRP):

7.22.1. תכנית היערכות להמשכיות עסקית (Disaster Recovery Plan) נועדה לסכל הפרעות לפעילות השוטפת של ממשל זמין ולהגן על נתונים מפני הרס, שיבוש, מחיקה וכדומה, הנגרמים בהשפעת מקרי כשל רציניים או מקרי אסון (שריפה, הצפה, אסונות טבע וכדומה), במערכות המידע הפיזיות והלוגיות של ממשל זמין.

7.22.2. באחריות הנהלת ממשל זמין למנות בעל תפקיד כאחראי על נושא ההיערכות להמשכיות עסקית.

7.22.3. בעל התפקיד, בתיאום עם מנהל מערך הסייבר ואבטחת מידע, יקבע את עקרונות ההיערכות להמשכיות עסקית של מערכות המידע בממשל זמין. עקרונות אלו יהוו תוכנית אסטרטגית, מבוססת על הערכת סיכונים נאותה, לטיפול כולל בהמשכיות תפעולית.

7.22.4. עקרונות ההיערכות יובאו לאישור ועדת ההיגוי העליונה, בטרם עיגונם בנהלים.

7.22.5. בעל התפקיד יפעל ליישום עקרונות ההיערכות להמשכיות עסקית ויהיה אחראי על תחזוקתה ועדכניותה של התכנית.

7.23. נהלים:

7.23.1. אחראי הסמכות ורגולציה אחראי לפיתוח נהלים לשם הסדרת פעילויות אבטחת המידע בממשל זמין.

7.23.2. אחראי הסמכות ורגולציה יהיה מעורב בפיתוח כלל הנהלים שיש להם השלכה על אבטחת המידע בממשל זמין.

7.23.3. נהלי אבטחת המידע חלים על כל עובדי ממשל זמין ועל ממשקיו באשר הם, אשר להם מעורבות בפיתוח, בתפעול, בתחזוקה, ביישום ובשימוש במידע.

7.24. הדרכה והטמעה של אבטחת המידע:

7.24.1. מנהל מערך הסייבר ואבטחת המידע יפעל להטמעת אבטחת המידע בכל מערכי המחשוב אשר בכל סביבות העבודה, בכלל מערכי התקשוב ובאמצעי העבודה הקשורים להיבטי האבטחה הפיזית ואבטחת הרשומות.

7.24.2. אחראי הסמכות ורגולציה יפעל להטמעת נהלי אבטחת המידע בתהליכי העבודה של ממשל זמין.

7.24.3. מנהל מערך הסייבר ואבטחת המידע יפעל להעלאת המודעות לאבטחת מידע בקרב עובדי ממשל זמין, ממשקיו והגורמים האחרים, להם נגישות למידע.

7.25. תוכנית עבודה ותקציב:

7.25.1. אחראי הסמכות ורגולציה יקיים דיוני עבודה ומעקב אחר ביצוע מדיניות אבטחת המידע.

7.25.2. אחראי הסמכות ורגולציה ואיכות ידווח תקופתית לוועדת היגוי לאבטחת המידע על פעילויות אבטחת המידע.

7.25.3. פעילות אבטחת המידע בממשל זמין תשולב בתוכנית העבודה השנתית והרב שנתית של ממשל זמין ותתוקצב בהתאם.

7.26. שיפור מתמיד:

7.26.1. דרישות לאבטחת מידע, ייקבעו על פי זיהוי סיכונים ודרישות התקנים. ממשל זמין יבצע סקר סיכונים מתודולוגי אחת לתקופה ולפיו ייקבעו הבקרות והתהליך להקטנת הסיכונים.

7.26.2. ממשל זמין יפעיל שיטת מדידה לעמידת ביצועי מערכת אבטחת מידע, אשר תאפשר למדוד את רמת האפקטיביות של ניהול אבטחת מידע והקטנת הסיכונים.

7.26.3. ממשל זמין יסקור אחת לשנה בסקר פנימי את תהליכי אבטחת המידע, על מנת להעריך את מידת ההתאמה של הנהלים להשגת המטרות.

7.26.4. תשומה של כל סקר פנימי, תועבר לתוכנית שיפור אשר תוודא שיפור מתמיד של מערכת אבטחת מידע. כל בעלי העניין יעודכנו אודות כל השיפורים שנעשו.

7.27. התאמה לדרישות שעל פי דין:

7.27.1. כל הדרישות הרלוונטיות שעל פי חוק, יוגדרו במפורש, יתועדו ויושמו עבור כל מערכות והיישומים של ממשל זמין.

7.27.2. כל השימוש בחומר שעשויות להיות לגביו זכויות קניין אינטלקטואלי ובמוצרי תוכנה קנייניים, ייעשה על פי חוק.

7.27.3. הגנת נתונים והגנת הפרטיות יובטחו כנדרש מתוקף הוראת חוק הגנת הפרטיות, התשמ"א 1981.

7.27.4. בקרות הצפנה יושמו בהתאם לכל ההסכמים, החוקים והתקנות הרלוונטיים.

8. נספח מערכות קריטיות

8.1. המערכות הקריטיות בממשל זמין הינן ככל המערכות המנגישות שירותים חיוניים - הן ללקוחות ממשל זמין (משרדי הממשלה ויחידות הסמך) והן אזרחי ישראל (כלל המשתמשים) – והן המערכות המאפשרות את הנגשת שירותים אלו ומגינות עליהם.

8.2. המערכות הקריטיות הינן אבני היסוד למילוי יעודו של ממשל זמין ולכן מערכות אלו יקבלו התייחסות מיוחדת לאורך כל מחזור החיים של המערכת – הן מבחינת שמירה על עקרונות אבטחת המידע בכלל (שלמות, אמינות, סודיות המידע) והן מבחינת ניהול והפחתת סיכונים, איכות ניהול המוצר (תיעוד), ושביעות רצון הלקוח בפרט.

8.3. בין המערכות החיוניות והקריטיות ניתן למצוא את שירותי התשלומים, הטפסים, חוות האירוח (אירוח אתרים) ובין המערכות המאפשרות את הנגשת השירותים ומגינות עליהם ניתן למצוא את מערכות הניטור והבקרה, מערכות אבטחת המידע, מערך האחסון וכיו"ב.

8.4. תפעול כל מערכת חיונית וקריטית נמצאת באחריות הצוותים הרלוונטיים במערך הסייבר ואבטחת המידע או מערך התקשורת וה-IT - כאשר פיתוח המוצר ואחזקתו נמצא באחריות מנהלי המוצר, מנהלי התחומים ומנהלי השירותים השונים בחטיבת המוצרים והשירותים בהתאמה.

8.5. במסמך ***אמנת השירות של ממשל זמין*** – והנספחים למסמך זה – מפורטים המערכות והשירותים הקריטיים אליהם תהיה התייחסות מיוחדת (גם מבחינת הסלמת הטיפול בתקלות בשירותים אלו). במסמך ***נכסי המידע של ממשל זמין*** מפורט הייעוד של כל מערכת קריטית ומפורטים בעליהן של המערכות הקריטיות. כפועל יוצא של הגדרות אמנת השירות והגדרת נכסי המידע, גם התשתיות המאפשרות את השירותים הקריטיים ומגינות עליהם נכנסות להגדרת המערכות הקריטיות של ממשל זמין.