היחידה להגנת
הסייבר בממשלה (יה"ב)

gov

רשות התקשוב הממשלתי
משרד ראש הממשלה

הנחיות ראש רשות התקשוב הממשלתי
הנחיות היחידה להגנת הסייבר בממשלה – יה"ב

שם ההנחיה: אבטחת מידע למעבר לענן ציבורי		
פרק ראשי: היחידה להגנת הסייבר בממשלה – יה"ב	מספר הנחיה: 5.5	תאריך הוצאה: 04.01.2017
פרק משני: שרשרת אספקה	מספר גרסה: 1.6	תאריך עדכון: 01.10.2017

אבטחת מידע

למעבר לענן ציבורי

תוכן עניינים

1. סמכויות היחידה להגנת הסייבר בממשלה (יה"ב)

בהחלטת הממשלה מספר 2443, מיום 15 פברואר 2015, נקבע כי ייעוד היחידה להגנת הסייבר בממשלה (יה"ב) הינו הכוונה והנחיה מקצועית בתחום הגנת הסייבר עבור כלל משרדי הממשלה ויחידות הסמך.
בדברי ההסבר להחלטת הממשלה נכתב כי הנחיות יה"ב מחייבות את משרדי הממשלה ויחידות הסמך.

2. קהל היעד

2.1. ממוני הגנת סייבר במשרדי הממשלה ויחידות הסמך.

2.2. מנהלי מערכות מידע במשרדי הממשלה ויחידות הסמך.

2.3. מנהלי אבטחת המידע והגנת הסייבר במשרדי הממשלה ויחידות הסמך.

3. מטרת ההנחיה

להנחות את קהל היעד בדבר התהליך הנדרש לצורך אישור בקשת משרד ממשלתי להעביר או להקים, מערכת מידע בענן ציבורי ולבאר למשרדים הממשלתיים את אופן הכנת מסמך הבקשה להעברה או להקמה, של מערכת מידע ממשלתית על גבי תשתיות ענן ציבורי.

4. הגדרות ומושגים

4.1. **רשות** – רשות התקשוב הממשלתי.

4.2. **יה"ב** – היחידה להגנת הסייבר בממשלה.

4.3. **הנחיה** – הנחית יה"ב במסגרת הנחיות ראש רשות התקשוב הממשלתי.

4.4. **משרד** - משרד ממשלתי או יחידה משרדית או יחידת סמך ממשלתית.

4.5. **יחידה מונחית רשות התקשוב** – יחידה בארגון המונחית על ידי רשות התקשוב הממשלתי בהתאם להחלטות הממשלה: אגף מערכות מידע, הגנת הסייבר, וכדומה.

4.6. **ממונה הגנת הסייבר** - אחראי במשרד לניהול והנחייה שוטפת בתחום הגנת הסייבר והנחלה של החלטות וסיכומי ועדת ההיגוי להגנת הסייבר.

4.7. **מנמ"ר (CIO)** - מנהל מידע ראשי (Chief Information Officer) / מנהל אגף מערכות מידע.

4.8. **ועדת ההיגוי לנושא הגנת הסייבר** – בכל משרד, אחראית לגיבוש עקרונות המדיניות, להתוויית אסטרטגיות לפעילות, לפיקוח אחר תכנית האב ותכניות העבודה השנתיות, לקיום הערכת נזקים בעקבות תקלות ולגיבוש המלצות לטיפול, על פי עקרונות מסמך המדיניות והמסגרת להגנה הסייבר הממשלתית.

4.9. **ענן מחשוב או מחשוב בענן (Cloud computing)** - שירותי מחשוב הניתנים למשתמש באמצעות שרתים מרוחקים, אליהם מתחבר המשתמש בד"כ באמצעות רשת האינטרנט.

4.10. **ענן ציבורי (Public Cloud)** - שירות המאחד מספר ארגונים (לקוחות) על תשתית מרכזית אחת.

4.11. **מחשוב ענן** - מודל מחשוב שבו תשתיות מחשוב (כוח מחשוב, זיכרון, בסיסי נתונים, שטח אחסון), יישומים, פלטפורמות לפיתוח יישומים, מוצעים לשימוש כשירות וניתנים לצריכה ותשלום ע"פ מודל שימוש, בתשלום (On-Demand), כאשר המשאבים המסופקים גדלים / קטנים עפ"י הצורך ועל פי אמנת שירות (SLA) מוסכמת.

4.12. **ענן פרטי** - מודל מחשוב בו לקוח הענן הוא היחיד אשר עושה שימוש בסביבת המחשוב.

4.13. **ענן קהילתי** - מודל מחשוב בו מספר ארגונים מסכמים על שימוש בתשתית מחשוב אחודה.

4.14. **ענן בן כלאיים (היברידי)** - מודל מחשוב בו עושים שימוש בשני סוגי עננים שונים (לדוגמה שילוב בין ציבורי לפרטי).

4.15. **מידע רגיש** - מידע אשר פגיעה בזמינותו, סודיותו או שלימותו עלולה לפגוע בניהולו התקין של המשרד הממשלתי או גופים אחרים.

4.16. **נתונים מותממים (Anonymized)** - נתונים אשר הוסרו מהם מאפיינים אשר יכולים להצביע על זהות האדם אשר מתואר בנתונים.

4.17. **נתונים ממוסכים (Masking)** - נתונים אשר שומרים על מבנה דומה לנתוני אמת אך אינם מכילים מידע אמיתי ואמין. מיסוך נתונים יכול להתבצע בצורה דינמית (המידע קיים בבסיס הנתונים אבל המשתמש לא חשוף לו) או סטאטית (בסיס הנתונים מעורבל ולא מכיל מידע אמיתי).

4.18. **מידע פרטי** - מידע הנתון להגנת חוק הגנת הפרטיות.

4.19. **דיירים (Tenants)** - הגופים השונים אשר מאכלסים את סביבת הענן. בענן ציבורי אין ללקוח שליטה על מי הדיירים החולקים את הסביבה ובענן פרטי לקוח הענן הוא הקובע מי הדיירים השונים.

4.20. **אישור ועדה** - הנחיה למנכ"לי המשרדים, ממונה הגנת הסייבר ומנהלי אגפי מערכות המידע במשרדי הממשלה ויחידות הסמך לפעול בשים לב לחוות דעת הועדה.

5. מבוא

5.1. רשות התקשוב הממשלתי תומכת במעבר לסביבת ענן ציבורי, מעצם העובדה כי שירותים אלה טומנים בחובם יתרונות משמעותיים למערך המחשוב הממשלתי, אך עם זאת יש לוודא כי אימוץ שירותי הענן נעשה באופן אחראי ותוך ניהול הסיכונים הרלוונטיים ובניית בקרות מתאימות.

5.2. כחלק מתהליך מעבר לסביבת ענן, פועלת רשות התקשוב הממשלתי לבחירת ספקים לשירותי ענן ציבורי העונים על תנאי- סף שהוגדרו על-ידי הרשות.

5.3. במסגרת מסמך זה יונחו משרדי הממשלה כיצד יש לבצע הערכת סיכונים ולממש את הבקרות הנדרשות במעבר לסביבת ענן.

6. איומים במחשוב ענן

טכנולוגיית מחשוב ענן טומנת בחובה יתרונות רבים למערך המחשוב, אך גם מגוון סיכונים אותם יש להעריך בעת מעבר לטכנולוגיה זו. חלק מהאיומים ייחודיים למחשוב ענן וחלקם מועצמים ע"י טכנולוגיה זו. בסעיפים הבאים יפורטו דוגמאות לסיכונים ותרחישי איום אשר יש לשקול את השפעתם בעת גיבוש החלטה על מעבר לסביבות ענן:

6.1. **חשיפה או זליגת מידע (Data breach):**

איומי חשיפה או זליגת מידע בסביבות ענן יכולים להיגרם כתוצאה ממספר תרחישים. להלן דוגמאות לתרחישים נפוצים:

6.1.1. חשיפת מידע כתוצאה מהפרדה לא יעילה בין לקוחות הענן (Tenants) החולקים את משאבי המחשוב.

6.1.2. חשיפת מידע עקב צו בית משפט של ממשלה זרה – שמירת מידע בתחום שיפוט שאינו מדינת ישראל, חושף את המידע לחוקים ותקנות של הממשלות בהם פועל ספק הענן ומאחסן את המידע. חוקים אלה שאינם בשליטת לקוח הענן יכולים לגרום לחשיפת מידע או לאי-זמינותו.

6.1.3. זליגת מידע עקב שימוש לא מבוקר בשירותי ענן – כאשר מידע רגיש ללא בקרות מתאימות מועבר לסביבות שלא ערוכות לאבטח נתונים אלו.

6.1.4. חשיפת מידע ע"י עובדי ספק הענן או צד שלישי בעל יכולת גישה למידע - מחשוב ענן, בדומה למיקור חוץ, מערב גורמים נוספים אשר אינם קשורים בקשר ישיר עם לקוח הענן ויתכן כי אינם מחויבים לחסיון המידע ולבעליו.

6.1.5. חשיפת מידע עקב אובדן או פריצה למכשיר קצה – מכשירי קצה רבים, לרוב מכשירים ניידים (Mobile Devices), עושים שימוש בשירותי ענן לצורך שמירת המידע במיקום מרכזי ונגיש. אובדן או סיכון מכשיר אשר אינו מוגן באמצעים הולמים יכול לגרום לחשיפת מידע.

6.2. **אובדן מידע (Data Lost):**

אחסנת מידע בשירותי ענן מגבירה לרוב את זמינות המידע. עם זאת, ספקי הענן אינם חסינים לאובדן (השמדה/שיבוש) המידע כתוצאה מתקלה או מפריצה למערכת שמלווה בהשמדת/שיבוש מידע. ככלל, יש לבחון את האיום של אובדן מידע (השמדת/שיבוש) תחת התרחישים הבאים:

6.2.1. אובדן המידע כתוצאה מתקלה אצל ספק הענן.

6.2.2. אובדן המידע עקב התקפה על החשבון או המערכת. יש לזכור כי במחשוב ענן הניהול המרכזי והיכולת לשלוט במגוון רכיבים ממיקום יחיד מגדילים את היכולת לפגוע בכלל המידע והרכיבים.

6.2.3. ספק הענן מפסיק את השירות.

6.3. **חטיפת חשבונות (Account or service hijacking):**

שירותי ענן שונים מהווים מטרה להשתלטות על חשבונות ממגוון סיבות - החל משליחת דואר זבל וכריית כסף וירטואלי וכלה בניסיונות סחיטה או איומים ישירים על הלקוח. תרחיש הכולל חטיפת חשבון יכול לגרום התממשות איום זליגת המידע או אובדן המידע, במקביל לסיכונים נוספים כגון אובדן מוניטין, פגיעה בזמינות, יצירת הוצאות כספיות או אובדן הכנסות.

6.4. **פגיעה בזמינות, שלמות או סודיות עקב ממשקי תוכנה וממשקי ניהול לא מאובטחים (Insecure interfaces & API):**

טכנולוגיות ענן כוללות לרוב מגוון רב של ממשקי ניהול המתאפיינים במגוון יכולות רחבות ממיקום מרכזי אחד, בדגש על שכבת API (Application Programing Interface) המאפשרת מגוון יכולות ניהול וגישה למידע. אי הגנה על ממשקים אלה עשויה לגרום להתממשות סיכונים כגון חטיפת חשבונות וזליגת מידע.

6.5. **אובדן זמינות המידע:**

בשירותי ענן זמינות המידע תלויה במספר גורמים וישנם מספר תרחישים אשר יכולים לגרום לאובדן זמינות השירות. הערכת הסיכונים צריכה לכלול התייחסות לתרחישים אלו:

6.5.1. ספק הענן אינו יכול לאפשר זמינות למערכת כתוצאה מתקלה או התקפה למניעת שירות.

6.5.2. לקוח השירות מאבד יכולת להתחבר למערכת כתוצאה מתקלה בחיבור לרשת או התקפה למניעת שירות.

6.5.3. חשבון הלקוח נחסם כתוצאה מתקלה, התקפה או הפרה של תנאי השירות.

6.5.4. ספק הענן מבצע השבתה יזומה.

6.5.5. ספק הענן אינו עומד בעומסים או ב – SLA הנדרש למימוש המערכת של הלקוח.

6.5.6. ספק הענן נאלץ להפסיק את השירות כתוצאה מצו בית משפט, הפרה של חוק/תקנות/החלטה עסקית/פיננסית.

6.6. **עלויות לא צפויות וסיכונים חוזיים וניהוליים:**

ארגונים רבים ממהרים לאמץ שירותי ענן כדי לממש את ההבטחה הגלומה בהם לחסכון הכספי, הורדת עלויות תפעוליות ויתרונות נוספים. כניסה חפוזה לשירות ענן ללא בדיקת איכות הספק ואיכות השירות הניתן על-ידו וללא הבנה מלאה של היקף המחויבות וחלוקת האחריות בין הספק ללקוח, עשויה לגרום להתממשות איומים כגון זליגת מידע, אובדן מידע ועלויות כספיות אשר לא תוכננו. להלן מספר דוגמאות לתרחישים:

6.6.1. הלקוח לא העריך נכון את כמות התעבורה, נפח האחסון או בקשות המידע למערכת המידע שלו ועל כן ישנו חיוב גבוה מהצפוי.

6.6.2. הלקוח ביצע טעות תפעולית או תכנונית אשר גורמת לחיוב כספי גדול מהצפוי. לדוגמה, אי כיבוי שרתים לתקופה ארוכה גורם לחיוב חודשי גדול מהצפוי.

6.6.3. הספק או השירות אינם עומדים ב – SLA ולכן זמינות או ביצועי המערכת נפגעים.

6.6.4. ספק הענן נקלע לבעיה עסקית וסוגר את החשבון או את השירות.

6.6.5. ספק הענן חוסם את חשבון הלקוח עקב סכסוך עסקי או משפטי.

6.7. **Vendor Lock in:**

ישנם מגוון סיבות שבעטיין ירצה לקוח להעביר את השירות שלו מספק הענן הנוכחי לספק ענן אחר או לרשת הפנימית. סיכון ה – Lock in עלול לגרום לכך שהעברה זו תהיה קשה ותכלול עלויות לא מתוכננות ואף אובדן מידע ו/או זמינות. בין הסיבות היכולות לגרום ללקוח לעבור לספק אחר ניתן לכלול:

6.7.1. ספק הענן אינו מספק שירות משביע רצון, אינו עומד ב – SLA או בהגדרות החוזה.

6.7.2. ספק הענן מפסיק פעילות, מעלה מחירים או מבטל שירות מסוים.

6.7.3. מערכת המידע משתנה וכוללת דרישות חדשות שאינן מקבלות מענה בסביבת ספק הענן הנוכחית.

7. תהליך המעבר למחשוב ענן במשרדי הממשלה

7.1. **כללי**

7.1.1. מובהר כי מדיניות רשות התקשוב הממשלתי היא לעודד יצירת שירותי ענן מקומיים, תוך עידוד השוק המקומי ושמירת המידע (ובכלל זה מידע על המידע, MetaData) בתחומי מדינת ישראל. על כן יינתנו הקלות בדרישות למעבר לספקי ענן מקומיים המקיימים את הדרישות המצויינות בנספח ה' במסמך זה.

7.1.2. משרד ממשלתי המבקש להקים מערכת ו/או להעביר מערכת קיימת לסביבת ענן ציבורי, יידרש לפנות לקבלת אישור ליה"ב, תוך הבהרת הסיכונים הנגזרים למשרד מתהליך המעבר לסביבת ענן.

7.1.3. יה"ב, בתיאום עם הגורמים הרלוונטיים, תהיה אמונה על אישור או דחיית הבקשות בהתאם לניתוח הסיכונים שיוצג על ידי המשרד.

7.1.4. במסגרת הבקשה שתוגש ליה"ב יעביר המשרד מסמך ייזום לצורך, אשר יוגש לאישור יה"ב, הכולל ניתוח של הסיכונים בהתאם לפורמט המצורף בנספח א'.

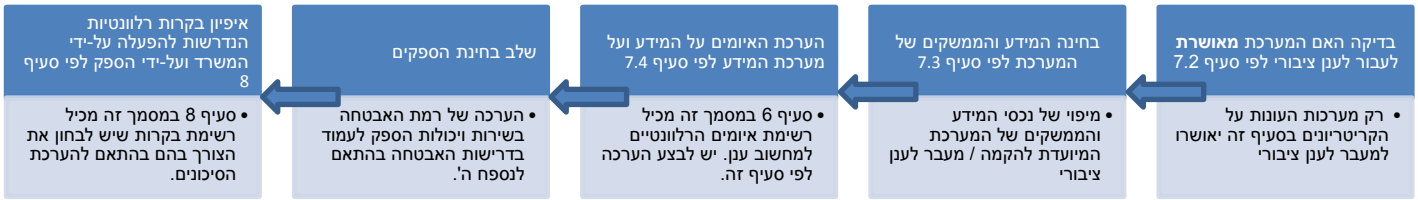
7.1.5. במסגרת המסמך שיוגש יוצגו הנתונים הבאים:

7.1.5.1. בדיקה האם המערכת מאושרת לעבור לענן ציבורי – לפי המוגדר בסעיף 7.2 להלן.

7.1.5.2. בחינת המידע והממשקים של המערכת – לפי המוגדר בסעיף 7.3 להלן.

7.1.5.3. הערכת האיומים על המידע ועל מערכת המידע – לפי בסעיף 7.4 להלן.

7.1.5.4. אפיון בקרות רלוונטיות הנדרשות להפעלה על-ידי המשרד ועל-ידי הספק – לפי המוגדר בסעיף 7.5 להלן.



7.2. **מערכות ומידע אותם מאושר להעביר לענן ציבורי:**

7.2.1. בהתאם למדיניות רשות התקשוב הממשלתי בשילוב גורמי מטה ממשלתיים נוספים, שימוש במשאבי ענן ציבורי יהיה באמצעות רשימת ספקי מחשוב ענן שייבחרו במכרז רשות התקשוב הממשלתי. ההיתר לשימוש בענן יתבצע לאחר בחינת ניתוח הסיכונים שיוצג ליה"ב.

7.2.2. לצורך קבלת אישור, על המערכות המיועדות לענות על כל המאפיינים הבאים:

7.2.2.1. מערכות אשר המידע בהן חשוף לציבור.

7.2.2.2. מערכות שאינן קריטיות.

7.2.2.3. מערכות שאינן מנהלות נתונים רגישים או חסויים.

7.2.2.4. מערכות שפגיעה בהן איננה מהווה פגיעה ביכולת המשילות של ממשלת ישראל ו/או בסמלי שלטון.

7.2.3. בנוסף, ניתן יהיה להעביר לענן ציבורי מערכות בשלבי פיתוח ובדיקות, אשר אינן כוללות לוגיקה חסויה והנתונים המנוהלים בהן אינם כוללים נתוני אמת, או שנתוני האמת בהם מותממים (Anonymized).

7.2.4. במידה ושירות הענן הנבחר הינו בתחומי מדינת ישראל ישקלו הקלות לקריטריונים הרשומים לעיל.

7.2.5. מערכות אשר קהל המשתמשים שלהן מורכב מעובדי מדינה הפועלים מחוץ לגבולות מדינת ישראל יבחנו, במידת הצורך, תחת קריטריונים מקלים.

7.2.6. העברת מידע המוגדר כרגיש בהתאם לחוק הגנת הפרטיות, התשמ"א-1981, לענן ציבורי מחוץ לגבולות מדינת ישראל, יעשה על-פי הנחיות רמו"ט (תמצית ההנחיות מצורפת בנספח ב').

7.2.7. על ספק השירות לציין בחוזה השירות כי סכסוך משפטי יתברר בתחומי מדינת ישראל ותחת חוקי מדינת ישראל (בהתאם לנספח ד').

7.2.8. משרד ממשלתי המבקש להעביר מערכת שאינה עומדת בקריטריונים המפורטים לעיל, אך סבור כי התועלת מהשירות גדולה מהסיכונים הצפויים, רשאי להגיש בקשה מנומקת לוועדה.

7.3. **שלב בחינת המידע והממשקים של המערכת:**

בשלב זה יתבצע ניתוח של המידע והמערכת המיועדת לעבור או להיות מוקמת בענן. בין הנתונים אשר יש לבחון:

7.3.1. סיווג הנתונים אשר ייכללו בסביבות הענן.

7.3.2. מיפוי המידע - האם חשוף לציבור? האם מכיל נתונים חסויים / רגישים? האם מכיל מידע רגיש לפי חוקי הגנת הפרטיות? האם הלוגיקה של היישום חושפת מידע חסוי / רגיש?

7.3.3. ממשקים - האם היישום משתמש בממשקים חיצוניים לרשת הפנימית? או בממשקים חיצוניים לספקים אחרים?

7.3.4. משתמשי היישום - מי הם משתמשי היישום? היכן הם מוגדרים? היכן הם ממוקמים? אילו הרשאות נדרשות מהמשתמשים השונים?

7.3.5. ספק התקשורת אל/מ ספק השירות הענני – מיהו הספק? מהם תשתיותיו? מהי רמת השירות המוגדרת (ובכלל זה הרמה ההגנתית)?

7.4. **שלב הערכת האיומים על המידע ועל מערכת המידע:**

טכנולוגיות ענן חשופות לאיומים שונים. חלק מן האיומים זהים לאיומים מסורתיים על מידע ועל מערכות מידע, וחלקם חדשים או מועצמים בהינתן טכנולוגיות הענן. הערכת האיומים שתוצג ליה"ב תכלול בחינה של הסעיפים הבאים:

7.4.1. האיומים הקיימים על המערכת המיועדת למעבר לענן, בהתחשב ברגישות המידע וסיכוני סודיות, זמינות ושלימות.

7.4.2. על המשרד לבצע תהליך הערכת סיכונים למערכת המידע ו/או למידע עצמו, תוך התייחסות לתהליכים ולמידע בהם נעשה שימוש ובהתאם לאיומים המתוארים בסעיף 6 לעיל. זאת, תוך דגש מיוחד על הסיכונים הבאים:

7.4.2.1. חשיפה של המידע לעובד של ספק הענן או צד שלישי.

7.4.2.2. חשיפת המידע לממשלות או גופי בטחון זרים.

7.4.2.3. סיכונים הנובעים מצווי בית משפט למידע המאוחסן אצל ספק הענן.

7.4.2.4. סיכונים הנובעים מחוסר שליטה מספקת על המידע.

7.4.2.5. סיכונים הנובעים מהעדר זמינות ספק הענן או המידע.

7.4.2.6. סיכונים הנובעים מחוסר בקרה וניטור מספק.

7.4.2.7. סיכונים הנובעים מנעילה (Lock-in) – חוסר היכולת להוציא את המידע מספק הענן.

7.4.2.8. סיכונים הנובעים מבקרות חסרות או שאינם מתפקדות כראוי אצל ספק הענן.

7.4.3. במסגרת שלב הערכת הסיכונים יש לזהות את הסיכונים הנותרים ללא מענה, לדרג את חשיבותם ולבדוק היתכנות ליישום בקרות משלימות על ידי הלקוח או צד שלישי.

7.5. **שלב הערכת הספק והשירות:**

7.5.1. מטרת שלב הערכת הספק היא לנתח את הסיכונים הנשקפים למידע מהספק והשירות אותו הוא מפעיל. סיכונים יכולים לנבוע מאופי הגוף המספק את השירות או מרמת אבטחת השירות. במסגרת שלב זה יש לבחון את מאפייני הספק כגון מהימנות, ניסיון, בגרות, משילות וסיכונים חוזיים ואת מאפייני השירות: בקרות אבטחת מידע שבשימוש, SLA והיכולת להגן על המידע.

7.5.2. אבן בניין מרכזית באסטרטגיית אבטחת מידע לשירותי ענן הוא הבנת מודל האחריות המשותפת (Shared responsibility model) ובו נקבעת חלוקת האחריות בין הספק ללקוח. על הלקוח להבין היטב את מבנה חלוקת האחריות אשר משתנה בהתאם לסוג השירות (תשתית, פלטפורמה או תוכנה כשירות) ותצורת הפריסה (ענן פרטי / היברידי / ציבורי/ קהילתי). בשלב זה יש לאפיין אילו בקרות אבטחת מידע הינם באחריות הלקוח ואילו באחריות הספק.

7.5.3. מימוש תהליך הבחינה של הספק יכול להתבצע במספר דרכים אשר יפורטו להלן. הדרך שבה יבחר לקוח הענן לבצע את ההערכה קשורה במישרין להערכת הסיכון לאפליקציה ויכולות ובגרות הספק. במידה והערכת הסיכון נמוכה ניתן להסתמך על הערכה עצמית של הספק, במקרה של אפליקציות קריטיות עדיפות לביצוע בחינה עצמאית של הספק בשילוב עם התחייבות חוזית. להלן השיטות המקובלות לבצע הערכת ספק:

7.5.3.1. הספק מבצע הערכה עצמית (Self-Assessment / Assertion) – בשיטה זו הספק מצהיר על קיומן של בקרות אבטחת המידע אשר הוא מפעיל, אך לא מספק מחויבות או בדיקה של צד שלישי לקיומן.

7.5.3.2. התחייבות חוזית לקיום הבקרות - בשיטה זו הספק מצהיר על בקרות אבטחת המידע ומספק התחייבות חוזית ברורה לקיומן. כולל SLA ודרכים למדוד את הביצוע לפי החוזה.

7.5.3.3. הסתמכות על הערכה / בחינה של צד שלישי – בשיטה זו ספק הענן מספק עדויות לכך כי מערך אבטחת המידע נבחן על ידי צד שלישי מהימן. בקטגוריה זו נמצאים גם ספקים אשר יספקו תעודת תאימות לתקנים כגון ISO 27001, SSAE 16 או CSA STAR. קיום הסמכות לתקנים אלה יכול להקל על מאמצי הבחינה והערכת הסיכונים.

7.5.3.4. ביצוע בחינה/הערכה עצמאית של הספק על ידי הלקוח או צד שלישי שמונה על ידי הלקוח.

ביצוע בחינה זו יכול לכלול:

- בחינה של הספק עצמו: חוזק פיננסי, ניסיון בשוק, מהימנות, בשלות, משילות, תאימות לתקנים.
- בחינה של מסמכים רלבנטיים כגון: חוזה, מדיניות אבטחת מידע, מדיניות גיבויים, נוהל התקנת טלאים, נהלי המשכיות עסקית והתאוששות מאסון.
- בחינה השירות עצמו: אלו בקרות אבטחת מידע נמצאות בשימוש? מהי היכולת של הלקוח לזהות אירוע חריג? לאיזה צד שלישי יש גישה למידע?
- ביצוע מבדקי חדירה (Penetration Test) על המערכת המוצעת לספק הענן. מבדקים אלה צריכים להתבצע לרוב בתיאום עם הספק ובהתאם להנחיותיו.
- ביצוע ביקורת של מערך האבטחה של ספק הענן ע"י ביקור באתר ובדיקה בפועל של קיום נהלים והנחיות.

7.6. **שלב אפיון בקרות רלוונטיות הנדרשות להפעלה על-ידי המשרד ועל-ידי הספק:**

7.6.1. כאמור, אבן בניין מרכזית באסטרטגיית הגנת הסייבר במעבר לשירותי ענן היא הבנת מודל האחריות המשותפת (Shared responsibility model) וקביעת חלוקת האחריות בין הספק ללקוח (נספח ג'). על המשרד לשקף הבנה של חלוקת האחריות, המשתנה בהתאם לסוג השירות (תשתית IaaS, פלטפורמה PaaS או תוכנה כשירות SaaS) ותצורת הפריסה (ענן פרטי/היברידי/ציבורי/קהילתי). בשלב זה יש לאפיין אילו בקרות להגנת הסייבר נמצאות באחריות הלקוח ואילו באחריות הספק.

7.6.2. לאחר איסוף הנתונים לגבי מערכת המידע, רישום, ניתוח והערכת האיומים ומיפוי היכולות של ספק הענן, ניתן לבצע הערכת סיכונים נכונה ולבצע מיפוי של הבקרות הנדרשות כנגד האיומים. שלב זה יכלול רשימת בקרות רלוונטיות להגנה על המידע. על הבקרות יצוין האם הנן באחריות המשרד המזמין או באחריות הספק, כיצד תמומש הבקרה, כיצד תיבחן יעילותה לאורך ההתקשרות והאם נדרשת רכישת תוכנה ו/או חומרה נוספת על-ידי המשרד לצורך הפעלתה.

7.6.3. בסעיף 8 להלן יוצגו בבקשה לאישור יה"ב בקרות אפשריות, בהתאם לסוג השירות ולסיכון הרלוונטי.

8. הנחיות הגנת הסייבר להקמת מערכות מבוססות מחשוב ענן

8.1. **כללי**

מטרת פרק זה לסייע לגופי הממשלה ליישם את דרישות הגנת הסייבר של יה"ב ולוודא כי שירותי הענן מוגנים בהתאם לסיכונים הנשקפים למידע ולמערכת המידע. באחריות המשרד למפות את הסיכונים כמפורט בסעיף 6 לעיל וליישם הגנה על המידע בהתאם לתפיסת הסיכון ולמדיניות הגנת הסייבר כמפורט בהנחיה זו.

מובהר כי ביצוע ניטור ובקרה על השירות הנו באחריות הבלעדית של המשרד.

בסעיפים הבאים תתבצע סקירה של בקרות מומלצות ליישום הגנה על המידע המועבר לשירותי ענן.

8.2. **משילות אבטחת המידע (Governance)**

8.2.1. משילות אבטחת המידע הינה אבן בניין מרכזית בבניית אסטרטגית ההגנה על שירותי מחשוב ענן. משילות נדרשת הן מצד לקוח הענן והן מצד הספק. הערכת משילות הספק הינה מדד הכרחי לבדיקת טיב השירות של ספק הענן עצמו וכלי מרכזי בהערכת הבשלות שלו ויכולתו לעמוד בדרישות SLA ואבטחת מידע.

8.2.2. על המשרד ליישם את מודל האחריות המשותפת (Shared responsibility model) הרלוונטי לשירות הענן הרלוונטי (כמפורט בנספח ג' להלן). במסגרת כתיבת הדרישות למערכת הענן יש למפות אילו בקרות הינן באחריות המשרד וכיצד ייושמו על-ידו ואילו בקרות הינן באחריות הספק.

8.2.3. בתצורות שירות IaaS ו – PaaS חלק גדול מהבקרות הנן באחריות המשרד. על-כן, על המשרד למפות את הבקרות הנדרשות להפעלה ישירה על-ידו, וככל שאינו מומחה בהפעלתן, להסתייע בכוח אדם מקצועי עם ניסיון רלוונטי לסביבות אלו. כמו כן, בתצורות IaaS ו – PaaS באחריות המשרד לבצע מבדקי חדירה וסריקת פגיעויות תקופתית על מערכות המידע הרלוונטיות.

8.2.4. בכל הנוגע למערכות SaaS הדרישה למבדקי חדירה תלויה בהערכת הסיכון שיבצע המשרד אל מול הבקרות המופעלות על-ידי הספק.

8.2.5. במידה והמידע המועבר לסביבות הענן מכיל נתונים הכפופים לחקיקה, תקינה או הנחיות אחרות – באחריות המשרד לוודא כי ספק שירותי הענן המציא מסמכים המעידים על עמידתו בדרישות.

8.2.6. על המשרד להעריך מהו הנזק העשוי להיגרם כתוצאה מאי זמינות השירות עקב תקלה או אירוע אצל ספק שירותי הענן או אי זמינות תשתית הגישה אל שירות הענן. בהתאם להערכת הסיכון יש לנקוט בבקרות מתאימות, כגון שימוש בקווי גיבוי, שמירת עותק מחוץ לענן או שימוש ביכולות שרידות והתאוששות מאסון (DR) (או כל בקרה אחרת מתאימה). הבקרות תיושמנה ברשת המקומית ו/או אצל ספק הענן או באמצעות שירות חיצוני.

8.2.7. על המשרד להעריך את יכולות ה – Governance של הספק, להלן מספר כלים אשר יכולים לסייע להערכה זו:

8.2.7.1. קיומו של בעל תפקיד בכיר אשר אחראי על נושא אבטחת המידע ומחויבות ההנהלה.

8.2.7.2. קיומם של נהלי אבטחת מידע כתובים וברורים המגדירים את תהליכי ניהול הסיכונים והבקרות הרלבנטיות.

8.2.7.3. תהליכים לזיהוי וציות לסוגיות משפטיות ורגולטוריות כולל הסמכות לתקנים ורגולציות.

8.2.7.4. בדיקות מהימנות של כוח האדם המועסק אצל ספק הענן (וקבלני המשנה שלו)

8.2.7.5. הפרדה בין תפקידי עבודה שונים לפי עקרון need to know.

8.2.8. פעמים רבות ספק ענן אינו פועל על גבי תשתית משלו אלא מסתייע בספקים אחרים ועל כן באחריות המשרד למפות את שרשרת האספקה על מנת לוודא כי לא חלים כשלים לאורך השרשרת.

8.2.8.1. על המשרד לקבל מיפוי מספקי שירות הענן לגבי חברות צד השלישי המשמשות אותם למתן השירות ואופן השפעתם על אבטחת השירות.

8.2.8.2. באחריות המשרד לוודא מול הספק הראשי כי גם ספקי המשנה כפופים חוזית להנחיות חוזיות

אשר נחתמות עם הספק הראשי בנושא אבטחת המערכת.

8.2.8.3. להלן דוגמאות לשאלות אשר יש לשאול כאשר בוחנים את נושא שרשת האספקה:

- האם המידע של הלקוח מועבר או נגיש לצד שלישי?
- האם ספק הענן מפעיל תהליך בחינה, סינון ופיקוח על ספקים?
- כיצד ספק הענן אוכף אל מול ספקי משנה את ההגבלות החוזיות אשר נחתמו עימו?
- לאילו תקנים ורגולציות כפופים ספקי המשנה?

8.2.9. עפ"י החלטת המשרד – יש לוודא יכולת לתרגל מצבי "שלילת יכולת" נקודתית ומערכתית.

8.2.10. רק ספקי שירות ענני העומדים בתקינה לאומית (ככל שקיימת) ובינ"ל מחייבת, כדוגמת ISO27001, ובדגש על סטנדרטים רגולטיביים מגזריים, יהיו מאושרים לספק שירותיהם לגופים במגזר הממשלתי.

8.3. מיקום גיאוגרפי ותחומי שיפוט

8.3.1. במחשוב ענן ישנה חשיבות גדולה למיקום הגיאוגרפי של שרתי המידע (לרבות גיבויי המידע ותשתית התאוששות מאסון) משום שחוקי ההגנה על המידע שונים בין תחומי שיפוט שונים. באחריות המשרד לבדוק באיזה תחום שיפוט נשמר המידע ע"י ספק הענן ולהביא העניין לידיעת יה"ב במסגרת בחינת הסיכונים שתיערך על-ידו.

8.3.2. כאשר המידע מאוחסן בתחום שיפוט מחוץ למדינת ישראל הוא אינו מוגן ע"י חוקי המדינה (נספח ד') ועל כן יש למפות מהי החקיקה הרלבנטית למקום בו המידע נמצא ולבצע ניתוח סיכונים לגבי חשיפה לצווי בית משפט או למערכות אכיפת החוק והמודיעין באזור האחסון.

8.3.3. כאשר המידע מאוחסן בתחום שיפוט שאינו מדינת ישראל יש לוודא כי החוזה שירותים עם הספק מכיל את ההגנות הנדרשות על המידע כולל הודעה ללקוח במקרה של צווי בית משפט בהתאם להנחיית היועמ"ש וכפי שמתואר בנספח ד' בהנחיה זו.

8.3.4. במידה והמידע המצוי במערכת המידע המשרדית כפוף לחוקי הגנת הפרטיות של מדינת ישראל, שמירת מידע תעשה רק בתחומי שיפוט המתאימים לפי הנחיות רמו"ט (נספח ב').

8.3.5. כמו כן, בכל הקשור למידע הכפוף לחוקי הגנת הפרטיות, על המשרד לוודא כי ספק הענן מסוגל להבטיח כי תחום השיפוט בו ישמר המידע לא ישתנה במהלך חיי ההתקשרות עמו. ככל שיודיע ספק שירותי הענן על כוונתו לשנות את תחום השיפוט בו יישמר המידע, על המשרד להביא הדברים לידיעת ר' יה"ב, כמפורט בהנחיה זו.

8.4. הגנה על מידע במנוחה (בזמן אחסון)

8.4.1. באחריות המשרד המזמין את שירותי הענן לוודא כי השירות המבוקש מכיל בקרות לגבי אופן הגישה למידע ויכולות ניטור ובקרה התואמות את אופי המידע ואת תפיסת הסיכון למערכת.

8.4.2. ספקי שירותי ענן מאפשרים הצפנת המידע בשכבות שונות של המערכת (לדוגמה הצפנת גיבויים, הצפנה ברמת בסיס הנתונים או ברמת שכבת האחסון). על המשרד המבקש ליישם את השירות, לבדוק אילו אפשרויות הצפנה קיימות בשירות והאם יישום ההצפנה מאפשר הגנה מפני מגוון האיומים הרלוונטיים למערכת.

8.4.3. בהתאם להערכת הסיכונים, על המשרד לשקול את האפשרות ליישם הצפנת מידע כאשר מפתחות ההצפנה ברשות המשרד.

8.4.4. במידת הצורך, ועל-פי אופי הנתונים, יש לשקול חלופות נוספות להצפנת המידע כגון מימוש טכנולוגיות

מסוג Tokenization, Masking או Anonymization.

8.4.5. יש לזכור כי בתצורות שירות כגון IaaS ו – PaaS, ביצוע גיבויים, התאוששות מאסון והמשכיות עסקית תלויה במידה רבה בארכיטקטורה שמיישם המשרד ומצויה באחריות המשרד, במסגרת חלוקת האחריות בינו ובין הספק.

8.5. **הגנה על מידע בתנועה (Data in Motion/Transit)**

8.5.1. בסביבות ענן ישנן מספר רשתות תקשורת טעונות הגנה:

8.5.1.1. תקשורת בין ספק שירותי הענן לרשת המשרד.

8.5.1.2. תקשורת בין ספק שירותי הענן למשתמשי הקצה.

8.5.1.3. תקשורת בתוך סביבת הענן (בין שרתים או שירותים).

8.5.1.4. תקשורת בין סביבת הענן לבין שירותים חיצוניים אחרים (לדוגמה API למערכות צד שלישי).

8.5.2. רשת התקשורת בין המשרד לספק שירותי הענן הנה באחריות המשרד. על-כן, על המשרד לוודא כי התקשורת בין המשרד לבין מערכות הספק מוצפנת בהתאם להערכת הסיכון.

8.5.3. על המשרד לשקול את הסיכון של אי-זמינות למערכת במידה ותהיה תקלה ברשת התקשורת שבאחריות המשרד ולהפעיל בקרות רלוונטיות בהתאם לסיכון.

8.5.4. בסביבות תשתית כשירות (IaaS), התקשורת בין השרתים של ספק הענן הנה באחריות המשרד. בהתאם להערכת הסיכונים יש לשקול להצפין גם תעבורה זו.

8.6. **הגנה על ממשקים**

8.6.1. ישנם סוגי ממשקים שונים אשר עשויים להיות מיושמים בסביבות ענן:

8.6.1.1. ממשק הניהול – ממשק הניהול של ספק שירותי הענן אטרקטיבי להתקפה, משום שלרוב הוא בעל הרשאות רבות, הפרדת תפקידים ברמה נמוכה וגישה ממגוון רשתות.

8.6.1.2. ממשקים בין המשרד למערכת הענן – מערכות ענן מסוגים שונים מקיימות ממשק לתוך הרשת הארגונית לצורך עדכון או משיכה של מידע.

8.6.1.3. ממשקי תמיכה ושירות – ממשקים אנושיים וממוחשבים אשר משמשים לתקשורת בין תמיכת הספק לאנשי המשרד.

8.6.1.4. ממשקים בין מערכת הענן לשירותים חיצוניים – ממשקים המקבלים או מוסרים מידע למערכות צד שלישי.

8.6.2. ממשק הניהול – על-פי רוב, נדרש להפעיל בקרות להגנת הסייבר אשר אינן מופעלות בתצורת ברירת מחדל ויש להפעילן בהתאם להערכת הסיכונים. בין הבקרות שיש לשקול הפעלתן:

8.6.2.1. הגבלת גישה אל ממשק הניהול מרשתות / ציודים מאושרים בלבד.

8.6.2.2. הצפנת התעבורה.

8.6.2.3. הפעלת יכולות זיהוי חזקה והפעלת בקרת גישה בהתאם לעקרון Least privilege role.

8.6.2.4. שילוב ניטור ובקרה מובנה הן לממשקים מבוססים GUI או ממשקי מכונה מבוססי API.

8.6.2.5. הפעלת מדיניות סיסמאות בהתאם לנהלי המשרד.

8.6.2.6. יישום נהלים לחילול, שמירה, שימוש נכון והחלפה תקופתית של API Keys ו – Host Keys.

8.6.2.7. ממשקים בין המשרד למערכת הענן – יישום הבקרות בממשקים אלה מצוי לרוב באחריות המשרד, בכפוף לאפשרויות הטכניות המצויות אצל ספק השירות. על מנת להקטין את הסיכון בממשק זה על המשרד לבחון את יישום הבקרות הבאות על-ידו:

8.6.2.8. בחינת טופולוגית החיבור כדי לזהות סיכונים.

8.6.2.9. שימוש בתקשורת מוצפנת והגבלת התקשורת במידת האפשר לטווחי כתובות ייחודיים והעדפה של ממשקים חד כיווניים.

8.6.2.10. שימוש בבקרות להקטנת הסיכונים (כגון שימוש במשתמש עם הרשאות, לקריאה בלבד, חיבור ספק הענן למערכת דמה או להעתק חיצוני).

8.6.2.11. ניטור ובקרה על פעולות הממשק, בין אם ממשק מבוסס GUI או ממשקי מכונה מבוססי API.

8.6.3. ממשקי תמיכה ושירות – על המשרד לוודא מול ספק הענן כי רק כוח אדם מאושר ומזוהה מראש יוכל לפנות לממשקי התמיכה לצורך קבלת השירות. יש לקבוע מראש את זהות מקבלי השירות ואופן ההזדהות.

8.6.4. ממשקים בין מערכת הענן לשירותים חיצוניים – מערכות עשויות להכיל ממשקים מבוססי API או תצורות נוספות על מנת לשאוב או לספק מידע למערכות חיצוניות של צד שלישי. ביישום ממשקים אלה על המשרד לוודא כי מתקיימות הבקרות הבאות:

8.6.4.1. הצפנה של תווך התעבורה.

8.6.4.2. שילוב אמצעי זיהוי בין הצדדים.

8.6.4.3. יישום מנגנון הרשאות.

8.6.4.4. תיעוד ובקרה של בקשות ומידע.

8.6.4.5. ביצוע של מבחני חדירה בהתאם לרמת הסיכון כדי לשלול קיום פגיעות מובנת בשירות.

8.6.5. לגבי כל סוגי הממשקים יש לבחון האם יש צורך לבצע מבחני חדירה על-מנת להעריך את רמת הסיכון. במידת הצורך, באחריות המשרד לבחון וליישם טכנולוגיות אבטחת מידע משלימות כגון:

8.6.5.1. שימוש ב – Web Application Firewall להגנה על ממשקים מבוססים Web.

8.6.5.2. שימוש ב – API Gateway לצורך הגנה על ממשקי מכונה למכונה.

8.6.5.3. שימוש בכלי זיהוי חדירות.

8.6.5.4. שימוש שוטף בכלי סריקה כדי לזהות חולשות חדשות.

8.6.5.5. שילוב של טכנולוגיות המונעות זליגת מידע דרך ממשקים אלה.

8.7. **אבטחת מידע אפליקטיבית (Application security)**

8.7.1. בתצורות שירות מסוג IaaS ו – PaaS קיום רמה נאותה של הגנה על מידע אפליקטיבי הינו באחריות המשרד. בין הבקרות השונות שבאחריות המשרד לבחון וליישם בהתאם להערכת הסיכון:

8.7.1.1. שימוש ב – Threat modeling עיתי הכולל התייחסות לסיכונים השכיחים בענן.

8.7.1.2. הגדרת דרישות לקוד מאובטח, ניהול מערכת ההרשאות ותאימות לתקינה.

8.7.1.3. שילוב של בדיקות מסוג Static analysis בעת הפיתוח.

8.7.1.4. שילוב של בדיקות מסוג Dynamic analysis בעת שלב הבדיקות והפריסה.

8.7.1.5. קיום של הפרדה מובנית בין סביבות פיתוח, בדיקות וייצור.

8.7.1.6. חתימה מאובטחת של יישומים ועדכוניהם.

8.7.2. בנוגע לכל תצורות השירות, שילוב כלים משלימים כגון סריקת חולשות, מבחני חדירה ושירותי Web Application Firewall, מצוי באחריות המשרד ונגזר מניתוח הסיכונים של מערכת המידע.

8.8. ניהול משתמשים והזדהות

8.8.1. אופן ההזדהות נקבע בין ספק שירותי הענן לבין המשרד, ובמקרים רבים מצוי באחריות המשרד. על המשרד המזמין את שירותי הענן לגבש את התפיסה הנכונה לניהול זהויות בהתאם לצרכים התפעוליים וצרכי אבטחת המידע.

8.8.2. בכל מקרה, כל הגישות למערכת, לרבות גישת לקוחות, קהל יעד, ספקי השירות, ספקי צד שלישי וגישת API לכל הממשקים, צריכות להיות מבוססות על זיהוי חד-ערכי, מוגבלות בהרשאות ומבוקרות בהתאם לצורך.

8.8.3. מדיניות הסיסמאות של מערכת הענן צריכה להתאים לנוהל הסיסמאות הקיים במשרד ועל פי דרישות ותקינה שהמשרד מחויב בהם.

8.8.4. על המשרד לבחון את האפשרות לניהול מרכזי של משתמשים באמצעות פרוטוקולי הזדהות מבוססי Identity Federation. שימוש בניהול מרכזי כאמור יאפשר למשרד לשלוט על זיהוי המשתמשים אצל ספק שירותי הענן ולמנוע סנכרון בין בסיס המשתמשים הפנימי לשירות הענן.

8.8.5. על המשרד לוודא כי הרשאות המשתמשים ניתנות בהתאם לעקרון Least privilege role וכי מודל ההרשאות תואם את הסיכונים הנשקפים למערכת.

8.8.6. מומלץ ליישם הזדהות חזקה מבוססת אימות כפול לפחות (2 Factor Authentication) של הישות המזדהה (אדם, מכונה, תהליך) בממשקי הניהול ועבור משתמשים בעלי הרשאות מיוחדות.

8.8.7. יש לתת דגש מיוחד ולהפעיל בקרות מפצות רלוונטיות בעת זיהוי משתמשים במערכות קצה ניידות (Mobile).

8.8.8. בסביבות PaaS ו – IaaS על המשרד ליישם מתודולוגיה מתאימה לחילול, שמירה והחלפה תקופתית של מגוון מפתחות ההצפנה המשמשים לגישה (API keys, Host keys).

8.9. תפעול מנגנוני הגנת הסייבר (Operational Cyber Security)

8.9.1. על המשרד לקבוע כיצד יישם את אחריותו על תפעול מנגנוני הגנת הסייבר. כאמור בסעיפים קודמים – ביצוע ניטור ובקרה על השירות מצוי תמיד באחריות המשרד. מעבר לכך ישנם נושאים תפעוליים רבים המצויים באחריות המשרד בהתאם לסוג השירות ותצורת השירות. בסעיפים הבאים יודגמו מספר נושאים שיש לתת דגש ביחס אליהם:

8.9.2. זיהוי וניהול אירועים

8.9.2.1. על המשרד להבין אלו מקורות לוג זמינים לזיהוי אירועים ומהם נהלי הספק בעת זיהוי אירוע.

8.9.2.2. באחריות המשרד לוודא כי אנשי הקשר אצל הספק לניהול אירוע אבטחת מידע, ידועים ומתועדים גם אצל ספק השירות וגם בקרב אנשי מערכות מידע של המשרד.

8.9.2.3. על המשרד לקבוע מהם תחומי אחריותו בעת ניהול אירוע ולשלב במידת הצורך כלים רלוונטיים כגון ביצוע Snapshot למכונה וירטואלית או כלים המאפשרים ניהול מצאי ואירועים בסביבות אלו.

8.9.2.4. במידת הצורך יש לבחון שילוב של כלי צד שלישי לצורך הגברת השליטה והגברת זיהוי אירועי כשל הגנתיים.

8.9.2.5. בהיעדר יכולת משרדית לזהות ולנהל אירועים – יש לדרוש מהספק הפנייה האירועים ל-SOC הממשלתי.

8.9.3. ניהול תצורה ושינויים

8.9.3.1. בסביבות IaaS ו – PaaS באחריות המשרד לתעד ולעקוב אחרי כל רכיבי התוכנה/ חומרה המעורבים בשירות ולוודא כי בידיו היכולת התפעולית לעשות כן.

8.9.3.2. על התיעוד לכלול את כל הנתונים הקשורים לתצורת הרכיבים השונים ואת הקשרים ביניהם וכמו כן לתעד שינויי תצורה.

8.9.4. ניהול טלאים ופגיעויות (Patch & Vulnerability Management)

8.9.4.1. בסביבות IaaS ובחלק מסביבות מבוססות PaaS על המשרד ליישם מדיניות של סריקת חולשות והטמעת טלאים על הרכיבים שבאחריותו.

8.9.4.2. מדיניות זו צריכה לכלול מנגנון לסריקת פגיעויות, תיעדוף תוצאות והתקנת טלאים בהתאם לרמת הסיכון.

8.10. **סיום השירות ומחיקת מידע**

8.10.1. על המשרד לוודא כי בכל זמן נתון ביכולתו לסיים את השירות ללא מגבלות חוזיות שאינן סבירות וכי נשמרת לו היכולת לייצא את המידע בצורה הניתנת לשחזור במערכת אחרת ותוך זמן סביר המוסכם בינו ובין הספק.

8.10.2. על מנת למנוע סיכוני נעילה (Lock-in) ניתן להפעיל את הבקרות הבאות:

8.10.2.1. תיעוד הממשקים וה – API אשר נעשה בהם שימוש.

8.10.2.2. ייצוא תקופתי של המידע מסביבת הענן לסביבה חיצונית, כולל Meta data רלוונטי.

8.10.2.3. בסביבות IaaS ו – PaaS יש מגוון כלים מובנים וכלים של צד שלישי המאפשרים לייצא את סביבת העבודה לסביבות אחרות.

8.10.3. באחריות המשרד לוודא כי חשבונות משתמשים והרשאות גישה ייחסמו לאחר סיום השימוש.

8.10.4. באחריות המשרד לוודא כי המידע ימחק בסיום השירות, וזאת על בסיס קבלת הוכחה מהספק על אופן הביצוע של המחיקה.

8.11. **מיפוי איומים כנגד בקרות**

8.11.1. מטרת הטבלה להלן הינה לתת אינדיקציה על הקשר בין האיומים / סיכונים המצוינים בפרק 6 כנגד הבקרות בפרק 8.

איום / סיכון	בקרות לפי פרק 8
חשיפה או זליגת מידע	• דגש על מיפוי סוג מידע העובר לסביבת הענן לפי סעיף 6.1 • סעיף 8.4 – הגנה על המידע במנוחה • סעיף 8.5 – הגנה על מידע בתנועה
אובדן מידע	• הערכה של מגוון אמצעי הגיבוי והמשכיות עסקית כולל יכולת לבצע גיבוי מחוץ לספק הענן • סעיף 8.4 – הגנה על מידע במנוחה • סעיף 8.9 – אבטחת מידע תפעולית
חטיפת חשבונות	• סעיף 8.6 – הגנה על ממשקים • סעיף 8.8 – ניהול משתמשים
ממשקים לא מאובטחים	• סעיף 8.6 – הגנה על ממשקים • סעיף 8.8 – ניהול משתמשים
אובדן זמינות המידע	• ניהול של מחויבות הספק במסגרת החוזה והתחייבות ל - SLA • סעיף 8.2 – משילות אבטחת המידע • סעיף 8.4 – הגנה על מידע במנוחה
אי הערכות נכונה	• ניהול בקרות משפטיות וניהוליות בחוזה מול ספק הענן • יישום סעיף 8.4 – ניתוח סיכונים במעבר לענן • סעיף 8.2 – משילות אבטחת המידע
סיכוני Lock in	• ניהול סיכונים בחוזה מול הספק • הגדרה מחייבת של מי בעל המידע ובעל הנתונים אודות המידע (Metadata) • קביעה חוזית של המידע ששייך ללקוח, כיצד ניתן לייצא אותו ואילו כלים יש לספק כדי לאפשר הוצאה זו • סעיף 8.10 – סיום השירות

9. מסמכים ישימים

9.1. מדיניות מימוש חזון מחשוב הענן במשרדי הממשלה, כפי שפורסמה ע"י רשות התקשוב הממשלתי.

10. רשימת נספחים

10.1. נספח א': בקשה להקמת מערכת בענן.

10.2. נספח ב': תמצית הנחיות רמו"ט בהעברת מידע אישי על ישראלים לעיבוד ממוחשב מחוץ לישראל.

10.3. נספח ג': מודל האחריות המשותפת (Shared Responsibility Model).

10.4. נספח ד': הנחיית היועץ המשפטי לממשלה - חוזים עם גורמי חוץ – תחולת החוק הישראלי.

10.5. נספח ה': דוגמה לרשימת דרישות עבור מכרז ענן ציבורי.

11. גרסאות ההנחיה

מס.	סטטוס	מהות שינוי	סעיפים שהושפעו	בתוקף מ –	נכתב ע"י	אושר ע"י
1.0	בתוקף	גרסה ראשונה		14.01.2016	ר' יה"ב	ר' רשות התקשוב הממשלתי
1.3	בתוקף	הערכת ספקים	8.2 , 7.5	01.12.2016	ר' יה"ב	ר' רשות התקשוב הממשלתי
1.4	בתוקף	תחום שיפוט מחוץ למדינת ישראל	8.3.3 , 8.3.2	01.05.2017	ר' יה"ב	ר' רשות התקשוב הממשלתי
	בתוקף	דוגמה לרשימת דרישות עבור מכרז ענן ציבורי	נספח ה'	01.05.2017	ר' יה"ב	ר' רשות התקשוב הממשלתי
1.5	בתוקף	הנחיית היועץ המשפטי לממשלה חוזים עם גורמי חוץ – תחולת החוק הישראלי	נספח ד'	01.07.2017	ר' יה"ב	ר' רשות התקשוב הממשלתי
1.6	בתוקף	עדכון תבנית	כל המסמך	01.10.2017	ר' יה"ב	ר' רשות התקשוב הממשלתי

12. נספחים

12.1. נספח א': בקשה להקמת מערכת בענן

תאריך	
שם המשרד	
מגיש מסמך זה	

המערכת	
שם המערכת	שם המערכת להתייחסות
תיאור פונקציונאלי	תיאור כללי - ייעוד המערכת, מטרות השימוש, קהל היעד
ארכיטקטורה	תיאור כללי - שרתים בכל הרמות, קישורים למערכות נוספות. עבור מערכות המפותחות ב - IaaS/PaaS.
מערכת חדשה	האם מדובר על מערכת חדשה, העברה של מערכת קיימת או שדרוג והוספת יכולות?

סוג המידע במערכת	**כן/לא**	**פירוט:**	**הסבר**
חשוף לציבור			האם הנתונים במערכת נגישים לציבור?
חשוף לספקים / קבלני משנה			האם הנתונים במערכת נגישים לגורמים חיצוניים?
מערכת קריטית			האם מוגדרת כמערכת קריטית?
סיווג בטחוני			האם קיים סיווג בטחוני למידע?
נתונים אישיים פרטיים			האם המידע מכיל פרטים מזהים על פי חוק ותקנות צנעת הפרט?
רגישות עסקית			האם המידע מכיל נתונים המשפיעים על התפקוד התקין של המשרד או הממשלה או העשויים לפגוע במשילות?

סוג המידע במערכת	כן/לא	פירוט:	הסבר
נתונים רפואיים			האם המידע מכיל נתונים רפואיים?
אחר			יש לפרט

ניתוח איומים כללי על המערכת	דירוג	פירוט
איומי זמינות	גבוה / בינוני / נמוך	
איומי שלמות	גבוה / בינוני / נמוך	
איומי סודיות	גבוה / בינוני / נמוך	

משתמשים	פירוט	הערות
סיווג המשתמשים		משתמשים פנימיים / חיצוניים? קבלני משנה? אזרחים?
כמות משתמשים		בחלוקה לפי משתמשים פנימיים, חיצוניים, קבלני משנה, אזרחים
מנהלי מערכת		כמה מנהלי מערכת יש? האם כולם עובדי המשרד? האם יש הבדל בין מנהלי המערכת השונים?
אופן הגישה למערכת		האם ניגשים רק מהמשרד המקומי או נדרשת גישה ממגוון מקורות? האם הגישה מבוססת דפדפן? האם נדרשת גישה ממערכות מובייל?
כיצד יוגדרו המשתמשים השונים		כיצד המשרד מתכוון לבצע ניהול משתמשים? תהליכי הוספה/גריעה? ניהול הרשאות?

משתמשים	פירוט	הערות
		סנכרון סיסמאות? האם ישנה כוונה ליישם Identity Federation?

ממשקים :

12.1.1. **פרט את סוגי הממשקים. כאשר לכל ממשק פרט את המידע הבא לכל הפחות:**

12.1.1.1. תיאור הממשק.

12.1.1.2. תדירות הקישור לממשק.

12.1.1.3. כיוון הממשק.

12.1.1.4. פרוטוקולים אשר בשימוש.

12.1.1.5. סוג ההזדהות.

12.1.1.6. האם לקריאה בלבד?

12.1.1.7. אם המערכת קיימת היום במשרד, אילו בקרות אבטחת מידע בשימוש :

	אמצעי הגנה	**פירוט**
אמצעי הגנה פנימיים	אופן ההזדהות למערכת	
	גישת מנהלי המערכת	
	הגבלת IP פנימית	
	הצפנות / חתימות	
	הזדהות ממשקים	
	אמצעי הגנה	**פירוט**
אמצעי הגנה חיצוניים	הגנה היקפית (Web / Database firewall)	
	מערכות HOST IPS	

פריט	תיאור
שם הספק	
שם השירות	
סוג השירות	
מיקום גיאוגרפי בו יישמר המידע	
מיקום גיאוגרפי של אתר משנה/ שירות גיבוי / התאוששות מאסון	
מדיניות אבטחת המידע של הספק	
תיאור כללי של הארכיטקטורה	

איום	פירוט	דוגמאות	דירוג הסיכון	בקרות שיופעלו						
			גבוה / בינוני / נמוך	הגנה על מידע במנוחה (בזמן אחסון)	הגנה על מידע בתנועה	הגנה על ממשקים	אבטחת מידע אפליקטיבית	ניהול משתמשים והרשאות	תפעול אבטחת המידע	סיום השירות ומחיקת מידע
זליגה או חשיפת מידע	**חשיפת מידע ע"י עובד של הספק**	עובד של ספקית שירותי ענן ניגש למידע חסוי אודות קטינים במערכת								
	חשיפת מידע עקב פריצה לחשבון או ניצול המערכת	ביצוע phishing או התקפה דומה על מנת לאפשר גישה לחשבון								
	צו בית משפט או תהליך גישת רשויות חוק	צו בית משפט אשר יוגש לספק המערכת לחשיפת מידע								
	חשיפה עקב אי שימוש לא מבוקר במערכת	עובד של חברת תרופות פרסם בטעות נתונים רפואיים של לקוחות לאחר שהעלה קובץ חסוי לתיקיה ציבורית בשירות אחסון קבצים								
אובדן מידע	**אובדן מידע עקב תקלה בשירות**	אלפי לקוחות של כל שירותי האחסון הגדולים חוו בשנים האחרונות איבוד מידע עקב תקלה								
	אובדן מידע עקב התקפה על המערכת	תוקף מחק את כל המידע של חברת תוכנה לאחר שהשיג גישה לחשבון דרך API Key אשר נשכח בטעות בקובץ הגדרות של התוכנה								
חטיפת חשבונות	**חטיפת חשבונות יכולה להביא לנזקי זמינות / שלימות / סודיות**	חשבונות דוא"ל מהווים מטרה נחשקת לחטיפה כי הם מאפשרים ביצוע SPAM בצורה קלה יותר								
ממשקי תוכנה וממשקי ניהול לא מאובטחים	**בסביבות ענן ישנם מגוון של ממשקים ויכולות ניהול באמצעות API. חשיפת ממשק יכולה להביא לנזקי זמינות / שלימות / סודיות**	חברת תוכנה סבלה מזליגת כל בסיס הנתונים של הלקוחות שלה עקב פגיעות ב - API של שירות התמיכה								

12.2. **נספח ב': תמצית הנחיות רמו"ט בהעברת מידע אישי על ישראלים לעיבוד ממוחשב מחוץ לישראל**

12.2.1. **אפשרות 1:**

12.2.1.1. ניתן לקבל שירות ענני - אם במדינה אליה מבקשים להעביר את המידע האישי קיימים דיני פרטיות, המבטיחים רמת הגנה על מידע, שאינה פחותה מרמת ההגנה על מידע, הקבועה בדין הישראלי.

12.2.1.2. רשימת המדינות:

- מדינות האיחוד האירופי.
- אנדורה.
- ארגנטינה.
- קנדה.
- שווייץ.
- איי פארו.
- גרנזי.
- האי מאן.

12.2.1.3. חובת בעל מאגר המידע, לקבל התחייבות בכתב מהספק, שהוא נוקט אמצעים מספיקים להבטחת פרטיות המידע, וכי המידע לא יועבר לאף אדם באותה מדינה או במדינה אחרת

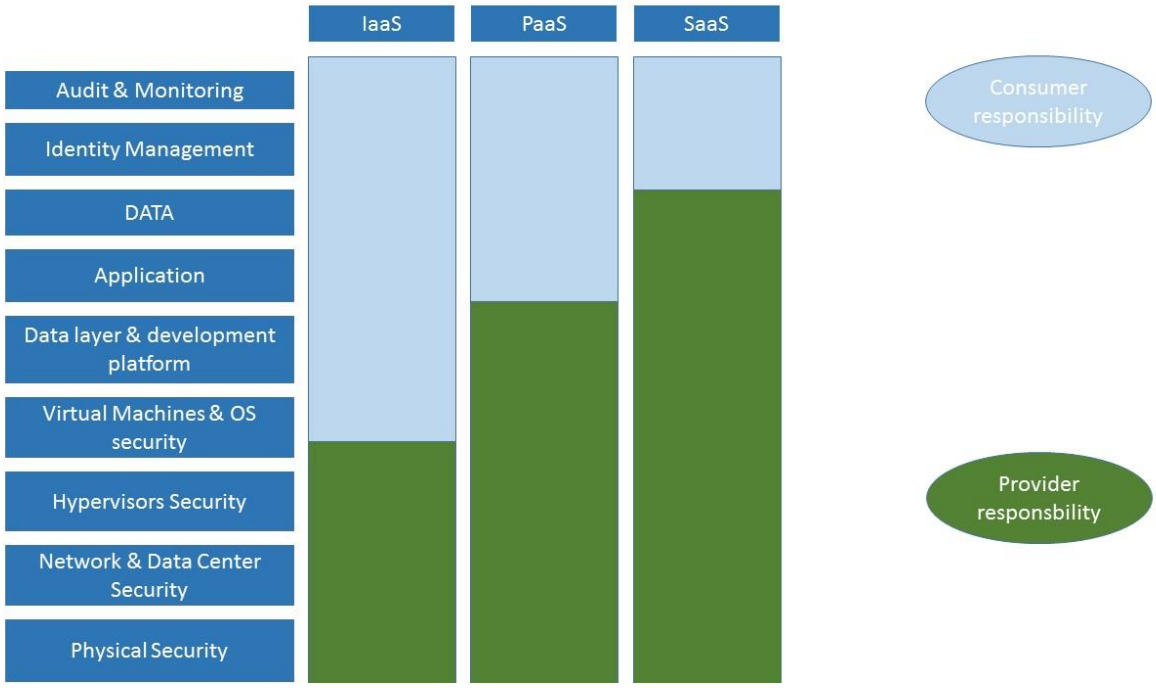
12.2.2. **אפשרות 2:**

12.2.2.1. ניתן לקבל שירות ענני באחת החלופות שלהלן:

- הגורם האחראי למידע ו/או למערכות שבאחריותו הסכים להעברה;
- לא ניתן לקבל את הסכמתו של האדם וההעברה הכרחית להגנה למידע ו/או למערכות שבאחריותו;
- המידע מועבר לתאגיד שנתון לשליטתו של בעל מאגר המידע והוא הבטיח את ההגנה על הפרטיות לאחר ההעברה;
- המידע מועבר למי שהתחייב בהסכם עם בעל מאגר המידע, לקיים את התנאים לאחזקת מידע ולשימוש בו החלים על מאגר מידע בישראל;
- המידע פורסם לרבים או הועמד לעיון הרבים על פי סמכות שבדין;
- העברת המידע הכרחית לשם הגנה על שלום הציבור או ביטחונו;
- העברת המידע מחויבת לפי הדין בישראל;

12.3. נספח ג': מודל האחריות המשותפת (Shared Responsibility Model)

מדיניות אבטחת המידע בסביבות הענן מבוססת על מודל האחריות המשותפת (Shared Responsibility Model).
מודל זה מגדיר כי במחשוב ענן ההגנה על המידע ומערכת המידע הינה אחריות אשר מתחלקת בין הספק ללקוח.
אופן חלוקת האחריות משתנה בהתאם לכל ספק וסוג שירות ועל כן יש לוודא עבור כל שירות את הבקרות אשר הינם באחריות הלקוח. עם זאת אפשר בצורה כללית להגדיר עבור תצורות השירות הנפוצות (SaaS/PaaS/IaaS) את חלוקת האחריות הבאה:



12.4. נספח ד' - הנחיית היועץ המשפטי לממשלה

חוזים עם גורמי חוץ – תחולת החוק הישראלי

1. בכל חוזה, הסכם או התקשרות אחרת (להלן – "חוזה") שבין המדינה או מוסד ממוסדותיה לבין גורם חוץ, תותנה התניה מפורשת שלפיה יחול על החוזה החוק הישראלי ושרק בית משפט ישראלי יהיה מוסמך לדון ולהכריע בכל הנוגע לאותו חוזה, פירושו או ביצועו וכל סעד הנובע מאי ביצועו או הפרתו.
2. לאור הנחיית היועץ המשפטי לממשלה, בכל חוזי הממשלה ככלל קיימת תניית שיפוט ישראלית.

12.5. נספח ה' – דוגמה לרשימת דרישות עבור מכרז ענן ציבורי

בנספח זה דוגמאות לסעיפי דרישות עבור מכרז שבו משתתפים ספקי ענן ציבורי עם דגש על שירותי תוכנה כשירות. יש להדגיש כי מדובר על רשימת דרישות אבטחת מידע כלליות שתפקידם לוודא כי הספק עומד בסטנדרט של אבטחת מידע התואם את ציפיות היחידה להגנת הסייבר בממשלה שברשות התקשוב הממשלתי. אין רשימת דרישות זו כוללת דרישות פונקציונאליות עבור המערכת שהיא נושא המכרז.

דרישות אבטחת מידע – ספק ענן

ספק שירות המבקש להציע במכרז פתרון במודל של שירות (As a service) אשר בו התוכנה מותקנת ומתופעלת בחצרות הספק יידרש לעמוד בסעיפים הבאים:

כללי:

1. השירות הנדרש יהיה מוסמך לתקן אבטחת מידע כגון ISO27001, SOC2 או תעודה מקבילה. הסמכת הספק תכלול את כל הרכיבים המעורבים בפתרון. יש לצרף עותק של תעודת ההסמכה למסמכי המכרז.
2. הספק יתאר או יצרף מסמך המתאר את מדיניות אבטחת המידע של השירות המוצע. הפירוט יכלול:
   2.1. תיאור הארכיטקטורה של המערכת המוצעת.
   2.2. בקרות אבטחת המידע אשר בשימוש המערכת החל ברמה הפיזית של הגנה על המערכת.
   2.3. נהלי גיבוי ו – DR.
   2.4. אופן פיתוח המערכת ושילוב SDLC במחזור החיים של המערכת.
   2.5. חלוקת תחומי אחריות אבטחת המידע (Shared responsibility module) בין היצרן ללקוח.
   2.6. תהליכים ארגוניים לצמצום סיכונים והתמודדות עם איומים.
   2.7. המצאות והערכה של תאימות לתקינה ולחוקים.
   2.8. אופן זיהוי ותגובה לאירועים.
   2.9. הערכת עובדים ובדיקות מהימנות.
   2.10. ביצוע מבדקי חדירה ו – Audit תקופתיים.
   2.11. יישום מנגנוני:
      2.11.1. הזדהות וניהול הרשאות.
      2.11.2. הצפנה של מידע בתנועה ומנוחה.
      2.11.3. ניטורים ולוגים הקיימים במערכת.
      2.11.4. זיהוי חולשות והתקנת טלאים.
3. במידה וספק המערכת עושה שימוש בתשתית מחשוב של ספק אחר, עליו לציין או לצרף מסמך המתאר כיצד מתבצעת חלוקת האחריות בינו לבין ספק התשתית ובאילו אמצעים הוא נוקט כדי להגן על המידע מפני הספק ומפני פגיעויות ברמת התשתית

שמירה ומחיקת מידע

4. באחריות הספק להגן על המידע אשר מאוחסן אצלו בהתאם להוראות החקיקה ודרישות המכרז. ההגנה כוללת ניתוח איומים, שערוך סיכונים וקביעת בקרות להתמודדות עם הסיכון.
5. הספק יפרט או יצרף מסמך המתאר את המיקום הגיאוגרפי בו נשמר המידע ותחומי שיפוט רלבנטיים.
6. הספק יפרט כיצד שמירת המידע עונה על חוק הגנת הפרטיות בישראל ותקנות רמו"ט לאחסון מידע פרטי.
7. הספק יפרט אילו בקרות ננקטות על מנת לוודא כי המידע אינו מועבר לתחומים גיאוגרפים אחרים.
8. הספק יפרט אילו אמצעי גיבוי קיימים בשירות בצורה מובנית וכיצד ניתן לבצע התאוששות מאסון.
9. הספק יפרט אילו אמצעי הצפנה קיימים על מידע במנוחה.
10. הספק יתחייב כי בתום השירות או לפי בקשה יימחק המידע של הלקוח ממערכות הספק, ללא יכולת שחזור של המידע – לרבות מידע על מידע (meta data) וכל דבר אחר הקשור לנתוני הלקוחות.

11. הספק יפרט כיצד מתבצעת מחיקה זו ואילו אישורים מתקבלים על כך.

ציות ומבדקים תקופתיים

12. באחריות הספק לוודא כי השירות המוצע עומד בדרישות התקינה שהוגדרו במכרז (הסמכת ISO27001 או SSAE SOC 2) לאורך תקופת החוזה.
13. באחריות הספק לוודא כי לאורך תקופת החוזה יתבצעו מבדקי אבטחת מידע תקופתיים מסוג Penetration tests ו – Vulnerability scan הכוללים בין השאר:
    a. בדיקות לתשתית .
    b. בדיקות של האפליקציה עצמה.
    c. בדיקות Social engineering או הדרכות מודעות לעובדים.
14. הספק ייפרט לאילו תקנות והסמכות השירות הוסמך, ויעמיד לרשות המבקש את תעודות ההסמכה.
15. הספק ייפרט כי הוא מבצע בדיקות תקופתיות אבטחת מידע תקופתיות, ייפרט את היקפן וטיבן והאם בכוונתו לספק תוצאות מבדקים אלה ללקוחות

אבטחה פיזית ובדיקות רקע

16. באחריות הספק לדאוג לאבטחת המתקן ממנו מופעל השירות ומתקני גיבוי.
17. אבטחת מתקן כוללת התמודדות עם איומים פנימיים, חיצוניים ואסונות טבע.
18. התמודדות עם איום פנימי כולל גם הגנה על המערכת מפני עובדים שסרחו או ספקי משנה המתחזקים את השירות.
19. חלק ממעגלי ההגנה של הספק להתמודדות עם האיומים יכלול בדיקות רקע לעובדים, אבטחת הגישה הפיזית ולוגית לשרתים, הפרדה בין תפקידים שונים וסביבות עבודה וכל הנדרש לפי התקנים המקובלים בשוק.
20. הספק יתאר או יצרף מסמך המתאר את הדרכים בהם הספק מתמודד עם איומים אלה.

ספקי משנה ואיומי שרשרת האספקה

21. באחריות הספק לנהל את האיומים הכרוכים בהתקשרות עם ספקי המשנה שלו, ולבצע ניתוח סיכונים על שרשרת האספקה שלוף
22. הספק יפרט אילו ספקי משנה מהווים חלק משמעותי בשירות והאם מידע של הלקוח מועבר לספקי משנה אלה.
23. הספק יתאר כיצד מתבצעת ההתמודדות עם איומים בשרשרת האספקה של השירות.

אבטחת מידע אפליקטיבית (Application Security)

24. השירות המוצע צריך להיות מפותח תוך שימת דגש על שיקולי אבטחת מידע ופרטיות.
25. על הספק לפתח את המערכת לפי סטנדרט SDLC (Security development life cycle) מקובל בשוק ויכלול הערכת סיכונים על האפליקציה (Threat modeling), הכשרת המפתחים בנושא א״מ, יישום בדיקות מסוג Static / Dynamic analysis וביצוע תקופתי של מבדקי חדירה.
26. הספק יפרט או יספק מסמך המתאר כיצד מבוצעת מתודולוגיית אבטחת המידע בעת הקמת המערכת

תפעול אבטחת המידע

27. תפעול השוטף של אבטחת המידע במערכת הינו באחריות הספק, תפעול זה כולל ניהול סיכונים שוטף של כל הרכיבים המשמשים לתפעול השירות החל מאבטחה פיזית של המתקן
28. הספק מתחייב כי הוא מתפעל את המערכת באופן שוטף כולל:

28.1. ביצוע של פעולות זיהוי של אירועי אבטחת מידע ותגובה.
28.2. תגובה לאירועי אבטחת מידע.
28.3. ניטור שוטף של המערכת לזיהוי תקלות ואירועים.
28.4. סריקה תקופתית לאיתור חולשות והתקנת טלאים בהתאם לנדרש.
28.5. גיבויים והערכות להתאוששות מאסון.
28.6. ניהול תהליך הערכת סיכונים תקופתי וכולל.

ערוצי תמיכה

29. על הספק לקיים מוקד תמיכה אשר יאפשר ללקוחות המערכת לבצע פניה בנושא תקלות או אירועי מערכת.
30. באחריות הספק לקיים הגנות על ערוץ תמיכה למערכת אשר ימנע שימוש לרעה בו ע"י משתמשים לא מורשים.
31. ההגנה על ערוצי התמיכה תכלול בין השאר
    31.1. נהלים מחמירים לגבי אופן הזיהוי של לקוחות המערכת,
    31.2. הדרכת העובדים לגבי התקפות מסוג Phishing / Social engineering .
    31.3. נהלים לגבי התנאים הנדרשים לבצע שינוי בשירות או לגשת למידע של הלקוח.
    31.4. בקרות, ניטור ובדיקה מדגמית / תקופתית על יישום הנהלים.
32. הספק יפרט כיצד בכוונתו לזהות את אנשי הלקוח בעת השימוש בערוצי השירות ואילו פעולות ננקטות על מנת למנוע מניפולציה של שירותי תמיכה לטובת התקפות סייבר.

ניהול אירועים

33. באחריות הספק לזהות אירועי אבטחת מידע בשירות, להתריע ללקוחות המערכת ולפעול לטיפול באירוע תוך שמירה על הסטנדרטים המקובלים בשוק
34. הספק מתחייב כי אירועי אבטחת מידע רלבנטיים ידווחו ללקוחות המערכת עם המידע הנחוץ.

כחלק מתהליך ניהול אירוע יש לשמור את כל המידע הרלבנטי כולל קבצי לוג, פעולות שבוצעו במערכת , תרחישי תגובה ומצבי מערכת (system state) לצורך ניתוח עתידי ועמידה בדרישות להתממשקות למערכת ניטור של המשרד / SOC ממשלתי.