מכרז פומבי מס' 02/2024 להקמת פלטפורמה טכנולוגית לאיגום המידע לתכנון, בנייה והקמת תשתיות בין גופי הממשלה

נספח ב9 - הנחיות אבטחת מידע

תוכן עניינים

1. **הקדמה** 3
2. **הנחיות אבטחת מידע בתהליכי התקשרות עם הספק** 4
3. **הגנה על המידע** 7
4. **הנחיות אבטחה פיזית בחצרות הספק** 9
5. **הגנה במערכות מידע** 10
6. **אבטחת ממשקים וממשקי ניהול** 10
7. **הקשחה** 11
8. **ניהול משתמשים וזהויות** (IAM/IDM) 11
9. **ניהול משתמשים וסיסמאות** 12
10. **תיעוד, לוגים וניטור** 12
11. **הנחיות כלליות לפיתוח מאובטח** 14
12. **הגנה בתהליכי הזדהות אפליקטיביים ומסדי נתונים** 17
13. **הגנה על מידע רגיש בבסיסי נתונים** 17
14. **הקשחת פרוטוקולים** 18
15. **אבטחת ממשקים אפליקטיביים** 20
16. **שימוש ב-** WAF/XMLFW 20
17. **שימוש ב-** API Gateway 20
18. **אבטחת שירותי** REST API 20
19. **הנחיות להקשחת שירותי** PUB/SUB 22
20. **הנחיות אבטחת-מידע לשימוש בקוד פתוח** (Open Source) 22

1. הקדמה

1.1. מטרה

1.1.1. מטרת מסמך זה להיות בסיס להנחיות אבטחת מידע להקמת פלטפורמה טכנולוגית לאיגום המידע לתכנון, בנייה והקמת תשתיות בין גופי הממשלה ורשויות באמצעות פלטפורמה מרכזית לשיתוף נתונים, תחקור וזיהוי חסמים בתחום התכנון והבנייה והתשתיות בתוך הממשלה (להלן: "**הפלטפורמה**"). הפלטפורמה אמורה לשרת מגוון גורמים ממשלתיים וציבוריים

1.1.2. מסמך זה על נספחיו הוא חלק בלתי נפרד מהמכרז.

1.2. היקף ומגבלות

1.2.1. מסמך זה והנחיותיו הם **<u>מנדטורי</u>**.

1.2.2. הנחיות אלה מתבססות על המסמכים הבאים מתוך הנחייה כי הספק יעמוד בהנחיות אלה בפתרון המסופק על ידו:

1.2.2.1. תורת הגנה בסייבר של מערך הסייבר הלאומי.

1.2.2.2. היחידה להגנה בסייבר (יה"ב).

1.2.2.3. תקנות הגנת הפרטיות (אבטחת מידע), תשע"ז-2017.

1.2.2.4. הנחית רשם מאגרי מידע מס' 2011/2 שימוש בשירותי מיקור חוץ **outsourcing** (לעיבוד מידע אישי) של הרשות למשפט וטכנולוגית מידע (רמו"ט).

1.2.2.5. הנחיות שימוש בשירותי מיקור חוץ (**Outsourcing**) לעיבוד מידע אישי.

1.2.2.6. עמידה בתקן **ISO27001**.

1.2.3. הספק יישא בכל עלות הנדרשת לצורך עמידה בהנחיות אלה וכתוצאה מאי עמידה בהנחיות מסמך זה וכן בכל עלות הנובעת משינוי, שיפור, או החרגה שנערכו לבקשתו.

1.2.4. המזמין רשאי להקל בהנחיות המסמך במקרים חריגים ובהתאם לשיקול דעתו הבלעדי. על הספק להיערך לעמידה בהנחיות כלשונן ולא תישמע טענה מצדו שלפיה סבר כי תינתן לו הקלה כלשהי. עם זאת, המזמין אינו מתחייב לאשר בקשות להחרגה או הקלה החורגות מנספח זה.

1.2.5. בסמכות המזמין לשנות מדרישות אבטחת המידע הנדרשות מהספק בעקבות אירוע סייבר או סיכון סייבר וכן לצורך מענה להנחיות חוק ורגולציה בנושא הגנת הסייבר.

1.2.6. הספק יהיה אחראי לאספקת השירות ולעמידה בהנחיות אבטחת מידע בכל הסביבות הטכנולוגיות.

2. הנחיות אבטחת מידע בתהליכי התקשרות עם הספק

2.1. מינוי נאמן אבטחת מידע

2.1.1. הספק ימנה נציג מטעמו (להלן: "**נאמן אבטחת מידע**"), שירכז את כל פעילויות הספק בהיבטי אבטחת המידע ויישא באחריות, בכל הנוגע לקיום הוראות פרק זה.

2.1.2. עד אישור המועמד לתפקיד נאמן אבטחת מידע ע"י המזמין, ייחשב מנכ"ל הספק כנאמן אבטחת מידע.

2.1.3. הספק יצרף כתב מינוי המסמיך את העובד המוצע לניהול אבט"מ במהלך כל תקופת ההתקשרות.

2.1.4. על מסמך הנחיות אבטחת המידע יחתום בנוסף למורשי החתימה גם ממונה אבטחת המידע ו/או ממונה הגנת הסייבר מטעם הספק. עובד זה יהיה גם גורם אחראי מטעם הספק לבקרה אחר יישום נספח ההנחיות ובכלל המערכות המשולבות בפלטפורמה.

2.1.5. לעובד שהוסמך לנושא אבטחת המידע תהיינה הסמכות רלוונטיות (תעודה) לניהול אבטחת מידע (**CISSP**) וניהול אבטחת מידע בענן **CCSK**, וכן הוא יהיה בעל ניסיון של 5 שנים לפחות בניהול פרויקטים דומים.

2.1.6. ממונה אבט"מ יצרף קו"ח והסמכות רלוונטיות להגנת הסייבר .

2.1.7. בחתימתו, מתחייב ממונה אבט"מ לפעול ולוודא יישום כלל הנחיות אבטחת המידע והגנת הסייבר המפורטות במסמך זה.

2.1.8. ממונה אבט"מ (ביחד עם מנהל הפרויקט) יהא מעורב באופן ישיר בכל שלבי הפרויקט ובין היתר יחתום גם על מסמכי התכנון, כמפורט בפרק 4 לנספח ב1 – השירותים הנדרשים. בחתימתו הוא מאשר את המסמכים, הטכנולוגיות ושיטות היישום עומדות בהנחיות מסמך זה ועומדים בהנחיות נספח זה.

2.1.9. הספק יעניק לנאמן אבטחת המידע סמכויות, כלים ואמצעים הנדרשים לביצוע תפקידו, לרבות סמכויות אכיפה וביקורת.

2.1.10. נאמן אבטחת מידע יקבל תדרוך מהמזמין לא יאוחר משבוע ימים ממועד מינויו.

2.1.11. על נאמן אבטחת המידע להיות בקיא בפרטי מכרז זה ונספח זה בפרט ובכל הנחיות אבטחת מידע המפורטים במסמך זה, החלים על הספק או מי מטעמו, ולאכוף אותם.

2.1.12. נאמן אבטחת מידע יקיים קשר שוטף עם המזמין האמון על נושא זה.

2.1.13. נאמן אבטחת מידע יתדרך ויעדכן את עובדי הספק בהוראות ובנהלים שיוגדרו בכל מהלך תקופת ההתקשרות.

2.2. ספקי משנה

2.2.1. המזמין רואה בספקי משנה של הספק (אלה שהוצגו במסגרת ההצעה ואלה שיאושרו על ידי המזמין לאחר הזכייה), כזרוע נוספת מטעם הספק. לפיכך, יחולו כל החובות וההנחיות המכרז גם על ספקי המשנה.

2.2.2. כל ההנחיות במסמך זה יחולו על הספק ועל קבלני המשנה, ככל ולא נאמר מפורשות אחרת. יובהר כי האחריות על קבלני המשנה לא תחול על קבלני משנה שהם יצרני כלי תשתית.

2.2.3. הספק הזוכה יעביר את רשימת כלל היצרנים והספקים שיהיו מעורבים בפעילות ואת תפקידם.

2.2.4. הספק הזוכה יישא באחריות ישירה לכל פער או סיכון הנובע משימוש בספקי משנה.

2.2.5. לא תינתן גישה למידע או מסירת מידע הקשור למכרז לספקי משנה ללא אישור בכתב של המזמין.

2.2.6. המזמין יהיה הגורם שיאשר כל גישת קבלן משנה למידע (פיזי או לוגי) וכן כל מעורבות של קבלן משנה אשר יהא מעורב בפעילות.

2.3. מהימנות כוח האדם

***הנחיות אלה יחולו על כל עובדי הספק הזוכה (שאינם ספקי מוצרי מדף וספק הענן) ובמהלך כל תקופת ההתקשרות שיהיו חשופים למידע לרבות אנשי מחשוב, מנהלה.

2.3.1. כל העובדים ,בין אם מדובר בעובדים הומוגניים של הספק ו/או עובדים של ספקי משנה מטעם הספק, יאושרו על ידי הגורמים שהוסמכו לכך על ידי המזמין.

2.3.2. הספק הזוכה יתחייב לקבל מראש ובכתב את הסכמת המזמין וראש תחום הגנת הסייבר של המזמין לגבי כל עובד מעובדיו ו/או מי מטעמו, המועסק בביצוע עבודות על פי מכרז זה. ראש תחום הגנת הסייבר של המזמין יהא רשאי לסרב לתת את הסכמתו להעסקת עובד פלוני של הספק הזוכה ו/או מי מטעמו מכל טעם שימצא לנכון, ומבלי שיהא עליו לנמקו.

2.3.3. כל העובדים (ידרשו בבדיקת רישום פלילי מול משטרת ישראל (טופס ר״פ) ובסיווג בטחוני רמה 5.

2.3.4. כל העובדים יחתמו על טופס התחייבות אישי לשמירת סודיות חסיון הנתונים ואי חשיפת מידע, מניעת ניגוד אינטרסים לרבות איסור להוצאה או מסירת מידע לגורם זר, העתקה, שמירה או צילום של מידע חסוי או רגיש בנוסח המצורף כנספח ב5 להסכם.

2.3.5. בעת שינוי במצבת כוח האדם, יעביר הספק מסמכים גם לעובדים חדשים אשר יצטרפו מטעמו לפעילות.

2.4. עמידה בהנחיות מערך הסייבר הלאומי לנושא שרשרת אספקה

2.4.1. לאחר הכרזה על הספק הזוכה, על הספק וגורמים המספקים לו שירותי פיתוח ואינטגרציה (בישראל בלבד ולמעט יצרנים של כלי תשתית בפלטפורמה) יוגדרו על ידי המזמין כ-**ספק רמה A** ויידרשו בביצוע סקר על בסיס השאלון העדכני ביותר למועד ההתקשרות, במערכת יעדים ובקרות לארגון (יוב״ל [1]) של מערך הסייבר הלאומי.

2.4.2. התהליך יבוצע באופן ממוקד **ורק** על השירות הניתן למזמין ולא על כלל שירותי הספק או שירותים אחרים שהספק מספק ללקוחות אחרים מטעמו.

2.4.3. מילוי הסקר במערכת יתבצע באמצעות בודק מוסמך מטעם מערך הסייבר הלאומי.

2.4.4. ככל שיעלו פערים במסגרת סקר זה, יידרש הספק לתקן את הליקויים בלוחות זמנים קצרים ככל הניתן שיקבעו בתיאום עם המזמין. לאחר תיקון הליקויים יבצע הספק סקר חוזר.

2.4.5. לאחר תיקון הליקויים, יגיש הספק את תוצאות הסקר לוועדת ההתעדה של מערך הסייבר הלאומי: (**https://www.gov.il/he/departments/news/querysupply**).

2.4.6. הספק יעביר את תוצאות הסקר ואישור וועדת ההתעדה, לראש תחום הגנת הסייבר של המזמין.

2.4.7. המזמין רשאי לדרוש מהספק לבצע סקר חוזר אחת לשנה וחצי.

2.5. סקר חצרות הספק(יבוצע על ידי המזמין)

[1] https://www.gov.il/he/departments/news/querysupply

***הנחיות אלה יחולו על הספק הזוכה (שאינם ספקי התשתית וספק הענן):

2.5.1. המזמין יהא רשאי לבצע סקר חצרות ספקים אשר יכלול בדיקות סקר סיכוני סייבר לספק ובין היתר בנושאי אבטחה פיזית, טכנולוגיות בהם הספק עושה שימוש לצורך הפרויקט ועוד.

2.5.2. עוד יבדקו פערים רגולטוריים, הגנת הפרטיות ונושאים המפורטים בנספח יוב"ל של מערך הסייבר הלאומי לרבות בדיקות טכנולוגיות מבססות.

2.5.3. הספק מחויב לתיקון ממצאים שיתגלו במסגרת סקר הספקים ובפרט ממצאים אשר עלולים לפגוע במזמין או במידע שלה בהיבטי סודיות, זמינות ואמינות.

2.5.4. הספק מסכים ומאשר כי ידוע לו כי יתכן שסקרים נוספים יוכלו להתבצע גם על ידי מערך הסייבר הלאומי ו/או מי מטעמו שהוסמך לכך.

2.5.5. הספק מסכים, כי ככל שיעלו ממצאים מהותיים (רגולטוריים, הגנת פרטיות או ממצאים טכנולוגיים החושפים את המידע של המזמין לסיכוני אמינות, סודיות או זמינות) יתחייב הספק לפעול לתקנם עד מועד אספקת השירות למזמין. תנאי זה הוא תנאי מנדטורי לעלייה לאוויר.

2.5.6. לאופן הטיפול יידרש הספק לספק אסמכתאות וכתב התחייבות החתום ע"י מורשה חתימה המפרט את אופן הטיפול בממצאים, וכן התחייבות כי ממצאי הסקר טופלו במלואם. ממצאים חריגים או חריגה מאופן טיפול הליקויים יובאו לאישור ראש תחום הגנת הסייבר במזמין ויהיו נתונים לשיקולו הבלעדי.

2.5.7. הספק מודע לכך כי עיכוב בתיקון הליקויים שיתגלו במסגרת תהליך הערכת הסיכון ו/או סקר חצרות ספקים, או מתן מענה חלקי לסיכונים שיתגלו, עלול למנוע ממנו מלספק או להמשיך לספק שירות למזמין וכן עשויים להוות הפרה של ההסכם ויחולו הוראות הרלוונטיות מהסכם ההתקשרות.

2.6. סקרי אבטחת מידע טכנולוגיים שיבוצעו על ידי הספק

2.6.1. על הספק לבצע סקר בטיחות (**Security Survey**), מבדקי חדירה (**Penetration Tests**), בדיקות קוד (**Code Review**) וסריקת חולשות (**Vulnerability Assessment**) בכל הסביבות בהן תותקן הפלטפורמה.

2.6.2. הסקרים יתבצעו במועדים הבאים:

2.6.2.1. סקר מלא – במסגרת שלב הבדיקות, כמפורט בסעיף 39 למפרט השירותים (נספח ב1 למכרז).

2.6.2.2. סקרים תקופתיים - במסגרת שלב התחזוקה, כמפורט בסעיף 53 למפרט השירותים (נספח ב1 למכרז). שיערכו בכל הסביבות (על פי תוכנית עבודה) הטכנולוגיות בהן קיימים שירותים או תהליכים המסופקים למזמין. במסגרת זו, כל הסביבות ידרשו להיבדק על ידי הספק לפחות אחת ל 18 חודשים.

2.6.3. תחולת הסקרים תתבצע למול הנחיות מסמך זה, המלצות היצרן להקשחת המערכות (**Best Practices**), ותפיסות הקשחה מקובלות רלוונטיות כגון: **CIS, NIST** ותורת ההגנה בסייבר לרבות: עדכניות המערכת, ניהול משתמשים, הרשאות, לוגים ואופן יישום המערכת בהתאמה לצורך הגנה שלשמה יושמה.

2.6.4. הסקרים יתבצעו על ידי גורם מומחה. הבדיקות תתבצענה לפני מסירת השירות למזמין על כל הסביבות אשר יוקצו עבור השירות.

2.6.5. הספק יפעל לטיפול בממצאים אשר יש להם השפעה על סיכוני אמינות, סודיות וזמינות בין היתר באמצעות עדכון הארכיטקטורה, רכש פתרונות אבטחה, ביצוע תהליכי פיתוח וכל פתרון רלוונטי הדרוש למענה לממצאי הבדיקות.

2.6.6. בכל המקרים בהם יתגלו ממצאים, יפעל הספק לטיפול בממצאים אשר יש להם השפעה על סיכוני אמינות, סודיות וזמינות בין היתר באמצעות עדכון הארכיטקטורה, רכש פתרונות אבטחה, ביצוע תהליכי פיתוח וכל פתרון רלוונטי הדרוש למענה לממצאי הבדיקות.

2.6.7. על הספק להעמיד לרשות המזמין את כל החומר והמידע שיידרשו ע"י המזמין ו/או נציגו, עפ"י שיקול דעתו הבלעדי של המזמין ו/או נציגו.

2.6.8. כמו כן, ביצוע הסקרים לא ישחרר את הספק מהתחייבויותיו ואחריותו כלפי המזמין למילוי ההנחיות וההוראות בנושא אבטחת המידע בהתאם לתנאי מכרז זה.

2.7. הפסקה ו/השהיית פעילות עם הספק בעת אי עמידה בנספח הנחיות אבטחת המידע

2.7.1. האחריות על עמידה בהנחיות ובדיקות אבטחת המידע וההגנה בסייבר וכן תיקון הליקויים ו/או סיכונים טכנולוגיים יחולו במלואם על הספק.

2.7.2. במקרה של אי עמידה בהנחיות נספח זה, ייחשב המצב כתקלה ויחולו ההוראות הקבועות בסעיף 85 לנספח ב1 – השירותים הנדרשים לעניין הדרישות מהספק במקרה של תקלה.

2.7.3. חידוש פעילות שהופסקה בעקבות סיכון סייבר תתאפשר רק לאחר שהספק ימלא אחר ההנחיות במלואן. רק ראש תחום אבטחת המידע של המזמין רשאי לאשר את חידוש הפעילות עם הספק וזאת רק לאחר שנבדקו על ידי המזמין או באמצעות בודק חיצוני מומחה - שייקבע על ידי ראש תחום אבטחת המידע של המזמין.

2.7.4. במקרה בו הספק לא יעמוד בהתחייבויותיו לנושא הגנת הסייבר או יסרב לתקן את הליקויים – יחולו הורות סעיף 21 בהסכם, לעניין הפרות הספק.

2.8. תקופת ההפרדות וסיום התקשרות עם הספק

2.8.1. מעבר לנדרש בהסכם ההתקשרות, בעת סיום התקשרות עם ספק, באחריות הספק לחסום ולהסיר את הרשאות הגישה אשר נפתחו במערכות הספק לעובדיו בפלטפורמה או בכל מערכת מידע רלוונטית אחרת.

2.8.2. באחריות הספק הזוכה להשיב כל מידע שנמסר למזמין לרבות מידע לוגי, פיזי, התקן מחשוב, התקן תקשורת, מודם סלולרי, התקן אימות זיהוי וכדומה.

2.8.3. הספק יצהיר במסגרת ההסכם כי הוא מחק, גרס, גרט ו/או השיב למזמין כל מידע אשר נמסר לו במסגרת מתן השירותים, בין אם מדובר במידע פיזי או לוגי לרבות מידע ממערכות מחשוב וגיבוי וכן כי נעשו תהליכי הסרת ההרשאות של הספק מהחשבון באופן שימנע שימוש של הספק בחשבון.

3. הגנה על המידע

3.1. כללי

3.1.1. כל פעילות הספק (פיתוח, עיבוד, אחסון, ניהול) במסגרת המכרז תבוצע בסביבת נימבוס **GCP** , בחשבון הייעודי שיוקצה לצורך הפלטפורמה, למעט במקרים חריגים אשר יאושרו מראש ובכתב על ידי ראש תחום אבטחת המידע של המזמין. בכל מקרה כזה נדרש הספק לפנות למזמין בכתב ולנמק את הצרכים ואמצעי ההגנה על המידע.

3.2. סוגי המידע בפלטפורמה

3.2.1. משרדי הממשלה וספקיהם מחויבים בתנאי שמירת סודיות. בין המידע שינוהל במסגרת הפלטפורמה יימצאו שני סוגי מידע ברמות הסיווג הבאות, בשירותי הענן:

3.2.1.1. מידע **עסקי לא רגיש בסיווג בלתי מסווג (להלן: "בלמ"ס")** של משרדי הממשלה השונים. מידע בלמ"ס יועבר באמצעים סטנדרטיים דוגמת דוא"ל משרדי בלבד של הספק או המשרד הממשלתי (אין לעשות שימוש בתיבות פרטיות (אישיות של עובד) שאינן משויכות לחשבון ניהולי (מותמם / אנונימי ושאינו מזוהה באופן ישיר עם המשרד).

3.2.1.2. מידע **טכנולוגי תפעולי** / **טכנולוגי רגיש** (לרבות: מידע תפעולי / שרטוטים / חשבונות / הגדרות רשת ומחשוב / כתובות **IP** / טכנולוגיות / הגדרות ניהול / לוגים ועוד) ומידע **עסקי רגיש** (תוכניות עבודה, תיקי תכנון ועוד) או **רגיש לפי תקנות הגנת הפרטיות(להלן ביחד: "מידע רגיש")**. בכל מקרה בו יוחזק, ינוהל או יעובד מידע רגיש על הספק להגן וליישם כלים ושיטות הגנה על מידע זה באמצעות השיטות הבאות:

3.2.1.2.1. ממשק מאובטח, דוגמת דוא"ל מאובטח, כספת או ממשקי **API** או **WEBSERVICE**).

3.2.1.2.2. זיהוי חזק (לדוגמה באמצעות תעודות אבטחה שיוגדרו בין כלל המערכות).

3.2.1.2.3. פרוטוקול מאובטח ומוצפן (לדוגמא **TLS 1.2-1.3**, **SSH**, **HTTPS** וכדומה).

3.2.1.2.4. באלגוריתם הצפנה חזק בעל מפתח ארוך (לדוגמה **AES-512** ומעלה).

3.2.1.2.5. ממשקי **API** / **WEB Service** (עפ"י נספח פיתוח מאובטח המצ"ב). ממשק **API** או **WEBSERVICE** מאובטח אשר יוקם בין המערכות.

3.3. הגנה על מידע בפלטפורמה לפי סביבות:

3.3.1. **סביבת הפיתוח (Dev)** - סביבה שתשמש את הספק לצורכי פיתוח וביצוע שינויים ושיפורים. ברשת זו לא ימצא מידע עסקי ומידע אישי רגישים, כפי שייקבעו כאלה על ידי המזמין או לפי דין. ככל שיעלה צורך, נתונים יהיו ללא פרטים מזהים. במידה ויהיה צורך בפעילות על נתונים רגישים הם יידרשו בהתממה.

3.3.2. **סביבת הטסט (QA)** – תשמש את הספק לצורך בדיקת גרסאות לפני העברתן לסביבת הייצור. סביבת הטסט תכלול נתונים לא רגישים. במידה וימצאו נתונים רגישים הם ידרשו בהתממה. רשת זו תכלול גם מערכות אבטחת מידע לבדיקות הדרושות במעבר בין סביבת הבדיקות לסביבת ייצור. ברשת זו לא ימצא מידע עסקי ומידע אישי רגישים. במידה והיה צורך בפעילות על נתונים רגישים הם יידרשו בהתממה.

3.3.3. **סביבת האינטגרציה (Staging)** - סביבה זו תשמש לצורכי הדרכה והטמעה. סביבת האינטגרציה תכלול נתונים מותממים. בסביבה זו ימצא מידע רגיש, והספק יידרש לפעול להגן על המידע מפני דלף וגישה לא מורשית.

3.3.4. **סביבת הייצור (Production)** - הסביבה תשמש כבסביבה התפעולית של הפלטפורמה. בסביבה זו ימצא מידע רגיש, והספק יידרש לפעול להגן על המידע מפני דלף וגישה לא מורשית.

3.4. שינוע ואחסון מידע

3.4.1. הספק לא יאחסן או יעביר מידע באמצעי אחסון או שינוע שלא אושרו על ידי המזמין לרבות: מצעי מדיה נתיקה (**Disk On Key, CD**, כונן קשיח נתיק) או במחשוב נייד (מחשב נישא, טלפון נייד, טאבלט) וכיו"ב.

3.5. הצפנה

3.5.1. תפיסת האגם, היא שהמידע הוא בלמ"ס ולכן לא יוצפן.

3.5.2. במידה ויוחלט להוסיף מידע לאגם שיוגדר כמידע רגיש או במקרים בהם שילוב מידע ממאגרים שונים יצרו מידע רגיש. המידע הרגיש יוצפן בסביבות הפלטפורמה והאפליקציות הרלוונטיות.

3.5.3. הספק יידרש לבצע בקרה על סוגי המידע ולהצפינם בהתאם לרמת הסיווג.

3.6. זיכוי מידע והלבנה

3.6.1. הספק יפעל על פי מדיניות **Zero Trust** בכל הממשקים בהם יתקבל מידע: הן במערכותיו ובכל הסביבות שפורטו לעיל. כמו כן, מערך הדיגיטל אמור ליישם מערך הלבנה בסביבת "שדרת המידע". ככל שלא תושלם הקמת מערך הלבנה בסביבת שדרת המידע, תחשב סביבה זו כסביבה בעלת סיכון, והספק יידרש לקיים הלבנה גם על קבצים המגיעים מסביבה זו.

3.6.2. הספק יבצע תהליכי הלבנה וזיכוי אבטחת מידע אפקטיביים, בכל ממשקי ותהליכי העברת מידע וקבצים כגון: מסביבה נמוכה (פיתוח) לסביבת ייצור, מסביבה חיצונית (אינטרנט, משרדי ממשלה) לסביבת הענן וכיו"ב.

3.6.3. על הספק למפות את כלל סוגי הקבצים הדרושים לקליטה ולספק להם פתרונות הלבנה, השטחה, **sandbox**, **CDR** מתאימים. קבצים אלה יוגדרו במדיניות **White List**. הספק יוכל לספק מענה להנחיות אלה באמצעות יותר מפתרון אחד.

3.6.4. על הספק למנוע הכנסת קבצים שלא אושרו במיפוי באמצעות יצירת חוקת **Black List**.

3.6.5. במקרים בהם לא ניתן ליישם פתרונות הלבנה. יציע הספק לקיים בקרות אבטחה וסינון תוכן אפקטיביים. לדוגמה: עבור קוד, יתבצע תהליך של **Code Review**, עבור כלי **Open Source** תתבצע גם בדיקת מהימנות למידע ואיתור חולשות / סיכונים הנובעים משימוש בכלים אלה.

3.6.6. הספק ימנע מהעלאת קבצים ממקורות לא מוכרים (משרדי ממשלה שלא אושרו, רשתות ומקורות זרים). ככל ויהיה צורך לעשות כן, יש לקבל אישור מראש ובכתב מהיחידה המקצועית.

3.7. הוצאה/פרסום מידע ופתרונות השחרה

3.7.1. ככלל, למזמין תהיה גישה לכל הסביבות, באופן שימזער את הצורך בהוצאת המידע אליו.

3.7.2. בכל העברת מידע מסביבת הייצור או האינטגרציה לסביבה נמוכה תתבצע בקרה על תוכן המידע למניעת דלף מידע שלא לצורך (רגיש או מידע תפעולי/טכנולוגי) בין היתר באמצעות התממת המידע.

3.7.3. הוצאת מידע מסביבת הענן לסביבות חיצוניות תתבצע על בסיס מנגנון ניהול הרשאות ואישורים אשר ינהל ויתעד את תהליך הבקשה למידע, אישור הבקשה וסוג המידע.

4. הנחיות אבטחה פיזית בחצרות הספק

***הנחיות אלה יחולו על הספק הזוכה (שאינם ספקי התשתית וספק הענן):

4.1. איסור אחסון מידע

4.1.1. כאמור לעיל, הספק לא יאחסן, ינהל או יעבד מידע בחצרותיו בשום אופן. עם זאת, הספק יוכל לעשות שימוש במשרדיו, עמדות מחשוב וסביבות מחשוב לצורך גישה למערכות הענן או לצורך ניהול פעילות הספק בפלטפורמה.

4.1.2. במקרה והספק כן יבקש לעשות שימוש באלה, הוא נדרש לפנות בכתב למזמין, לנמק את הצורך ולקבל את אישור המזמין.

4.1.3. הספק יעבור סקר אבטחה פיזית על ידי המזמין ויידרש לקיים את הבקרות שיועברו לו על ידי המזמין דוגמת:

4.1.3.1. נהלים ומדיניות ומודעות עובדים להגנה ואבטחה פיזית.

4.1.3.2. לקיים תהליכי הגנה, אחסון ובקרת גישה למידע בין היתר באמצעות: יצירת אזורים מאובטחים וממודרים, בקרת כניסה ומצלמות אבטחה ואמצעי ניטור אפקטיביים לניטור גישה פיזית שאינה מורשית.

4.1.3.3. יישום מצלמות אבטחה- הספק נדרש לוודא צילום רציף 24/7/365 ועמידה ובתקנות הגנת הפרטיות ויכולת תחקור ויזואלית של עד חצי שנה.

4.1.4. הספק יבצע ביקורות אבטחה פיזית מעת לעת לתקינות אמצעי הבקרה והתראה (אזעקה) וסדרי הדיווח בגין אירוע פיזי.

5. הגנה במערכות מידע

5.1. יישום מערכות אבטחת מידע בתקשורת

5.1.1. הספק יגדיר את מערכות התשתית בתצורה אשר תאפשר סגמנטציה ברמה הנמוכה ביותר (**Layer2**) האפשרית. במקרים בהם לא ניתן ליישם הפרדת **Layer2**, תתבצע הפרדה באמצעות **Layer3** דרך רכיב ניטור וסינון תוכן דוגמת: רכיבי אבטחה: **Firewall** בעלי יכולות אבטחת מידע (**IPS, Antivirus, URL Filtering, Antimalware, AntiSpoofing, Content Inspection**), מערכת הגנה אפליקטיבית **WAF**, שרתי ניהול משתמשים, הפצת עדכונים, ניטור אבטחת מידע, טלפוניה וכיו"ב.

5.1.2. כל הממשקים האפליקטיביים החיצוניים ינוטרו באמצעות מערכות **WAF**.

5.1.3. הספק יוודא הפרדה מלאה בין ממשקי ניהול לבין ממשקי **Data** וממשקי עבודה עסקיים.

5.2. יישום כלי אבטחת מידע בתוך מערכות/סביבות

5.2.1. הספק נדרש לוודא כי כל הפתרונות המסופקים על ידו ימוגנו באמצעות כלי הגנה מתאימים לפני עלייה לייצור.

5.2.2. הספק יישם אמצעים לגילוי, התרעה והסרה של וירוסים ותוכנות זדוניות בכל סביבות העבודה. לפיכך, כל רכיב תוכנה אשר יושם בפתרון ימוגן באמצעות כלי אבטחת מידע אשר יאפשרו: זיהוי וניתוח סיכוני סייבר על בסיס חתימות ואנומליה, כגון: **EDR** או **XDR**.

5.2.3. הספק נדרש לוודא כי כל הפתרונות המסופקים על ידו ימוגנו באמצעות כלי הגנה אפקטיביים לפני עלייה לייצור.

5.3. יישום אמצעים לאיתור אנומליה והטעיה

5.3.1. הספק יקים פתרונות אפקטיביים לאיתור אנומליה והטעיה (דוגמת מלכודות דבש ופתרונות **Honey Token**) שיש עימה להשפיע על רמת ההגנה בסייבר בכל הסביבות סגמנט או סביבה ויאפשרו זיהוי והתראה על פעילות מסוכנת או חריגה.

5.3.2. במסגרת השגרות השוטפות, נדרש הספק לבצע בקרות על התראות ממערכות אלה ולטייב אותן במטרה להתאימן לאיומים להן הם נועדו לתת מענה.

6. אבטחת ממשקים וממשקי ניהול

6.1. הגנה על ממשקי ניהול

6.1.1. הספק יישם הפרדת ממשק הניהול של כלל המערכות מממשקי השירות והאפליקציה.

6.1.2. הגישה לממשקי הניהול תתאפשר רק מרשתות ישראל תוך: זיהוי הרשת (**IP**) ממנה מתבצעת ההתקשרות, זיהוי חד ערכי של המשתמש, וזיהוי המחשב ממנו מתבצעת הגישה.

6.1.3. גישה לממשק ניהול תעשה בפרוטוקולי ניהול מאובטחים ומוצפנים. ככלל בכל ממשק ניהול והעברת מידע, יעשה שימוש בפרוטוקולים מאובטחים ומוצפנים ובעלי מפתחות ההצפנה ארוכים.

6.1.4. במקרים בהם יהא צורך בפענוח הפרוטוקולים לצורך ניטור התעבורה באמצעי אבטחת המידע, יבחנו שיטות לניהול המפתחות במערכות הניטור או יישום טרמינציה לפרוטוקול (לדוגמה: **SSL Inspection**).

6.1.5. הגישה לממשק הניהול של המערכות יתאפשר באמצעות ניהול משתמשים וקבוצות משתמשים על פי קבוצות הרשאה (קריאה בלבד, עריכה חלקית, עריכה מלאה).

6.1.6. אימות משתמשי הניהול יעשה מול מערכת ניהול הזהויות ותשתיות סטנדרטיות לניהול מרכזי של משתמשים.

6.1.7. הזדהות משתמש תוך מתן הזדהות חזקה **2FA** או **MFA**.

6.1.8. כל פעולות הניהול יתועדו במלואן, בין אם הסתיימו בהצלחה או בכישלון.

6.1.9. הספק יפנה התראות על גישה לממשקי הניהול בערוץ מוצפן ל- **SOC** הממשלתי.

6.2. ניהול תעודות אבטחה בממשקי ענן ומול משרדי הממשלה

6.2.1. עבור כל כתובת חיצונית החשופה לאינטרנט וכן בכל ממשק תקשורת לשירות חיצוני יעשה שימוש בתעודות אבטחה שיירכשו לצורך כך על ידי ספק מנפיק תעודות מוסמך.

6.2.2. בין שרתים ושירותים אפליקטיביים פנימיים בשירותי הענן ושירותים פנימיים (דוגמת ממשקי **API**) יוגדרו תעודות אבטחה פנימיות.

6.2.2.1. הפקה וניהול המפתחות יתבצע באמצעות שירות **KMS/HSM/CA** של ספק שירותי הענן.

6.2.2.2. הספק יקיים אמצעי הגנה למניעת דלף או גישה של גורם לא מורשה (גם מחצרות הספק/ענן) לתעודות.

7. הקשחה

7.1. כללי

7.1.1. על הספק לוודא כי כל רכיב טכנולוגי (לרבות: שירות, אפליקציה, מערכת הפעלה, מחשוב אישי, שרתים, מערכות הפלטפורמה ועוד) אשר ישמש לצורך פעילות הפרויקט והפלטפורמה, יוקשח על בסיס **Best Practices** מקובלים, כגון: **CIS Benchmark** והמלצות היצרן ברמה המחמירה ביותר האפשרית, שאינה פוגעת בתהליך העסקי.

7.1.2. כל תהליכי ההקשחה יתבצעו ממקום מרכזי (סביבת ניהול) ובאמצעות כלי הקשחה (ובקרת הקשחה) ייעודיים. כלים אלה יאפשרו גם בקרות (התראות ודוחות) על שינויים בהקשחה, לרבות אירועים חריגים.

7.1.3. הבקרה על טיב ההקשחה תיבדק באמצעות כלי סריקת החולשות, סקר סיכונים, ובדיקות החדירות. הספק יידרש לתקן כל ליקוי אשר יזוהה כפער הקשחה – כל עוד הוא אינו פוגע בתהליך העסקי.

7.1.4. חריגים בהקשחה או חריגים שלא הוקשחו עקב פגיעה בתהליך עסקי, יועברו לידי המזמין לצורך בחינתו וקבלת החלטתו.

7.2. שימוש בפרוטוקולי ניהול מאובטחים

7.2.1. גישה לממשקי הניהול של רכיבי התקשורת תהיה באמצעות פרוטוקולי ניהול מוצפנים ומאובטחים המצריכים אימות זיהוי (דוגמת: **HTTPS, SSH, SFTP** ו- **SNMP V3**).

7.2.2. הגישה לממשקי הניהול תתאפשר מסביבת הניהול בלבד.

7.2.3. הספק ישנה ערכי ברירת מחדל (חשבונות ניהול, סיסמאות וכיו"ב) לערכים ייעודיים אחרים בהתאם למדיניות הסיסמאות המפורטת במסמך זה.

8. ניהול משתמשים וזהויות (IAM/IDM)

8.1. הנחיות בנושא זה מפורטות בסעיף **21** במסמך המכרז.

9. ניהול משתמשים וסיסמאות

9.1. הנחיות בנושא זה מפורטות בסעיף **20** במסמך המכרז.

10. תיעוד, לוגים וניטור

10.1. ניטור מקומי במערכות ואפליקציות

10.1.1. בכל המערכות: תשתית, מע' הפעלה, מע' הגנה בסייבר והאפליקציות, יתאפשר ניטור מקומי של אירועי אבטחת מידע, סייבר ואירועים תפעוליים.

10.1.2. המערכות ישמרו לוגים בתצורה מקומית למשך תקופה של חודש לכל הפחות. במידה ולא יעשה שימוש במערכת איסוף מרכזית, **על כל מערכת (תשתית, סיסטם, אבטחת מידע) או אפליקציה לשמור לוגים מקומית לתקופה של 24 חודשים** אלא אם המזמין אישר לספק לפעול אחרת.

10.1.3. לוגים המיוצרים על ידי האפליקציה, יישמרו בבסיס נתונים נפרד המשמש למטרה זו בלבד.

10.2. ניטור אירועי אבטחת מידע

10.2.1. על הספק להתקין שרת **Collector** בכל סביבה לאיסוף הלוגים.

10.2.2. הלוגים יועברו למערכת ה- **SIEM** של ה-**SOC** הממשלתי על בסיס הנחיות שיועברו לספק על ידי ה- **SOC** הממשלתי.

10.2.3. על הספק להגדיר את כלל המערכות והאפליקציות (לרבות מערכות הגנה בסייבר) עליהן נדרש לדווח את התראות ל- **SOC** הממשלתי.

10.2.4. ככל שיידרש, הספק יסייע בטיוב ההתראות והאירועים בשיתוף ה- **SOC** הממשלתי.

10.2.5. הספק מתחייב לנטר את הלוגים ממערכות אלה ולדווח ל- **SOC** הממשלתי על פעילות חריגה או מסוכנת.

10.2.6. יש לשמור את הלוגים בבסיס הנתונים או בשרתי איסוף לוגים **(Collector)**. אלא אם המזמין אישר לספק לפעול אחרת.

10.2.7. הניטור יתבצע במשך כל ימי השבוע, 24 שעות ביממה ויאפשר יכולת תגובה מהירה במקרה של אירוע אבטחה.

10.2.8. הניטור ויכולת התגובה ימשכו כל זמן ההתקשרות עם המזמין.

10.2.9. שליטה וצפייה בפעולות החריגות המערכת יתבצעו דרך ממשקי הניהול השונים המאפשרים צפייה בלוגים אפליקטיביים במערכת מתוך רשת ניהול ייעודית שתוגדר בסביבת העבודה של הספק המיועדת למזמין (רשת ניהול בסביבת מערכות המזמין בחצרות הספק).

10.3. שעון אחיד

10.3.1. בכל השירותים שמוגדרים כ- **Compute Engine** יוגדר שעון אחיד **(NTP)**.

10.4. בקרה אחר פעולות משתמשים

10.4.1. יש לקיים בקרה (לוג) אחר כל פעילות המבוצעת על ידי משתמשים החשופים לסביבת מערכת ניהול לרבות כל משתמש: אנונימי, מזוהה, מזוהה חזק, אפליקטיבי, בסיס נתונים ומשתמשים ניהוליים **(administrators, system admins)**.

10.5. ניטור משתמשי תהליכים **(Services)**

10.5.1. יש לוודא ניטור מלא על כל פעילות משתמשי **Services**.

10.5.2. יש לייצא התראות על התנהגות חריגה, למשל חשבון **Service** המנסה להפעיל **Service** אחר ממה שהוגדר לו.

10.6. תיעוד ולוגים (התראות) ממערכות ההגנה בתקשורת

10.6.1. כל הלוגים יתעדו מועד: שעות, דקות, שניות, ותאריך.
10.6.2. נתוני התיעוד של מנגנון הבקרה יישמרו גם בסביבה מקומית במערכת למשך 24 חודשים לפחות אלא אם המזמין אישר לספק לפעול אחרת.
10.6.3. תיעוד לוגים עבור ממשקים ומערכות:
10.6.3.1. מזהה רשת: כתובת ה- **IP**, **MAC**, שם רכיב, פורט תקשורת.
10.6.3.2. מזהה משתמש (אנושי/אפליקטיבי) וסוג ההרשאה (קריאה, כתיבה).
10.6.3.3. מזהה היישום.
10.6.3.4. בעת גישה לקבצים: שם הקובץ והפעולה שנעשתה (שינוי לפני ואחרי).
10.6.3.5. התראות בגין שינויי הגדרות בכל אחד מרכיבי הרשת והשרתים.
10.6.3.6. התראות בגין תקלה או פגיעה במערכת או בסוכן.
10.6.3.7. כמות הפניות.
10.6.4. תיעוד לוגים עבור ממשקים חיצוניים:
10.6.4.1. בפניות תקשורתיות - כתובת **IP** אשר תזהה את מקור הפנייה, פורט תקשורת.
10.6.4.2. בפניות אפליקטיביות - סוג ומבנה השאילתה.
10.6.4.3. בפניות אנונימיות - אפליקציה באמצעותה בוצעה הפנייה.
10.6.4.4. בפניות מזוהות – חשבון המשתמש באמצעותו בוצעה הפעולה, לרבות חשבון המשתמש.
10.6.4.5. כמות הפניות.
10.6.4.6. תקלות זמינות.
10.6.4.7. עומסים חריגים.
10.7. תיעוד פעולות חריגות
10.7.1. יש לתעד את הפעולות הבאות:
10.7.1.1. שליפת מספר רב של מידע (סף קבוע מראש) או שליפה החורגת מהנורמה (אנומליה).
10.7.1.2. מחיקת מידע.
10.7.1.3. פעולות ניהול במערכת.
10.7.1.4. גישה לבסיס הנתונים.
10.8. לוגים תפעוליים
10.8.1. את תיעוד הלוגים יש ליישם באמצעות מנגנון מובנה לרישום לוגים.
10.8.2. עבור כל לוג יש לרשום את:
10.8.2.1. פרטים מזהים (חד ערכיים) על מבצע הפעולה.
10.8.2.2. כתובת **IP** ממנה בוצעה הפעולה.
10.8.2.3. זמן ביצוע הפעולה – תאריך, שעה, דקה ושנייה.
10.8.2.4. מהות הפעולה / סוג הפעולה.
10.8.2.5. ערך ישן (לפני שינוי) וערך חדש (אחרי שינוי).
10.8.2.6. סטטוס הפעולה (הצלחה, כישלון).
10.8.3. יש לתעד מידע תפעולי ואבטחת מידע באופן המקסימלי האפשרי.
10.8.4. יש לתעד את האירועים הבאים:
10.8.4.1. גישה ללוגים.
10.8.4.2. קריאת מידע רגיש.
10.8.4.3. מחיקת מידע.
10.8.4.4. ביצוע זיהוי ראשוני וביצוע זיהוי חוזר באמצעות **OTP**.
10.8.4.5. ביצוע **Logout** במערכת.
10.8.4.6. ניסיון הזדהות כושל.
10.9. ניהול הרשאות גישה ללוגים.

10.9.1. יש לצמצם את הרשאות הגישה ללוגים למנהלי המערכת בלבד.
10.9.2. צפייה בלוגים.
10.9.2.1. גישה ללוגים תתבצע ע"י גישת **UI** דרך מסך ייעודי המשמש למטרה זו ונגיש לגורמים מורשים בלבד (המזמין או רשת ניטור ייעודית של הספק).
10.9.2.2. גישה למסך זו תאופשר למנהל המערכת בלבד.
10.9.2.3. אין לאפשר או להסתמך על גישה ישירה לבסיס הנתונים למטרה זו.
10.9.3. יש למנוע יכולת מחיקה או שינוי לוגים – גם לבעלי הרשאות גבוהות (מנהלי המערכת).

10.10. התראות
10.10.1. עבור כל רישום של לוג של פעולה חריגה במערכת יש לייצר התראה.
10.10.2. ההתראה תישלח לקבוצת אנשים מוגדרים באמצעות אי-מייל או **SMS** המציין שקיימת פעילות חריגה במערכת.

10.11. דוחות
10.11.1. הספק יוודא כי מערכת הניטור תייצא דוחות בתדירות יומית, שבועית וחודשית לכל אורך זמן הפעילות במטרה לאתר שינויים בהתנהגות.
10.11.2. הדוחות יכללו את נושאים הבאים:
10.11.2.1. דוחות סיכום.
10.11.2.2. דוחות שינויים בהגדרות:
10.11.2.3. חוקה: יצירת חוקה חדשה, שינויים בחוקה קיימת, הסרת חוקה, עצירת חוקה (**disable**).
10.11.2.4. משתמשים: יצירת משתמש חדש, יצירת משתמש ניהולי, שינויים בהרשאות.
10.11.2.5. הספק מתחייב לנהל בקרה ומעקב אחרי דו"חות ומגמות עבור איתור אירועים חריגים , דיווח וטיפול בהם. הספק, אם יידרש יציג את דו"חות אלה למזמין, במועד העברת הדרישה.

10.12. טיוב התראות
10.12.1. במסגרת השגרות השוטפות, נדרש הספק לבצע טיוב מחזורי ההתראות ולטייב אותן.

10.13. גיבוי
10.13.1. יש לבצע גיבוי תדיר ומסודר באמצעות העברת הלוגים לסביבת גיבוי דרך ממשק מאובטח.
10.13.2. במסגרת השגרות השוטפות, נדרש הספק לבצע בדיקות מדגמיות לבדיקת תקינות גיבוי הלוגים.

11. הנחיות כלליות לפיתוח מאובטח

הערה: הנחיות בנספחים 19-21 יחולו בכל תהליך בו יתבצע פיתוח תוכנה או יעשה שימוש בכלי Opensource.

11.1. כללי
11.1.1. כלל תהליכי הפיתוח יתייחסו **גם** לסיכונים מתוך **OWASP Top 10:2021**, **OWASP API Security Top 10:2023** ו- **OWASP Top 10 CI/CD Security Risks** **(או העדכני ממנו במהלך כל תקופת אספקת שירותי הפיתוח).**
11.1.2. כל תהליכי הבדיקות יעשו בסביבת רשת הבדיקות.
11.1.3. כל חלק קוד/ רכיבי תוכנה צד שלישי יהיו ממקורות מהימנים בלבד לאחר אישור היחידה המקצועית.

11.1.4. לאחר רישום משתמש או אימות זיהוי מחדש של משתמש חוזר, יוצג למשתמש פרטי המשתמש, מועד הכניסה האחרון (אם בוצע), וכן שעון ותאריך עדכניים של מועד הכניסה העדכניים.

11.2. בדיקות קלט

11.2.1. בדיקות קלט אשר מתקבלים ממשתמשים הן מהיסודות החשובים ביותר של אבטחת מידע בתחום האפליקטיבי והמקור העיקרי לבעיות רבות בתחום זה. משתמש זדוני ינסה להזין קלט לא חוקי או מסוכן יש לוודא שהמערכת מסוגלת להתמודד עם כל סוגי הקלט האפשריים.

11.2.2. חובה לבצע בקלט בדיקה חיובית (**White list check**) – כלומר להרשות רק תווים ומחרוזות שמותר (בניגוד למניעת מעבר של תווים אסורים).

11.3. הנחיות לבדיקות קלט

11.3.1. יש לוודא כי בדיקות הקלט מתבצעות הן בצד הלקוח והן בצד השרת. אין להסתמך על בדיקות תקינות המבוצעות בצד הלקוח.

11.3.2. עבור כל בדיקת קלט שנכשלה יש לוודא כי הבקשה נכשלת ונשלחת הודעת **HTTP Response – Bad Request**. ניתן לציין את הסיבה לכישלון ברמה העסקית אך אין לחשוף מידע טכני מיותר.

11.3.3. יש לבצע את בדיקות הקלט במערכת במנגנון מרכזי אחד שיהיה אחראי על בדיקות הקלט במערכת.

11.3.4. עבור כל קלט במערכת יש לבצע בדיקות קלט באמצעות הגדרת **Whitelist** בה מגדירים מהו ערך תקין ורק אותו מאפשרים. עבור כל קלט יש להגדיר את הבדיקות הבאות:

11.3.4.1. האם נדרש או לא (**Required**).

11.3.4.2. אורך הקלט – הגדרות מינימום ומקסימום.

11.3.4.3. סוג הקלט – **String, Integer, Boolean** וכו'.

11.3.4.4. **Regular Expressions** – יש להגדיר עבור שדות טקסט.

11.3.5. בנוסף לשיטת ה - **Whitelist**, יש לעשות שימוש בשיטת **Blacklist** בה מגדירים ערכים לא תקינים ולא מאפשרים אותם. יש לסנן את הקלטים הבאים:

11.3.5.1. פקודות **JavaScript**, פקודות **SQL**, פקודות **HTML** וכו'.

11.3.5.2. יש לבצע **Encoding** לכל מידע שמוצג למשתמשים שמקורו ממשתמשי מערכת.

11.3.5.3. השאילתות לבסיס הנתונים יבוצעו באמצעות **Stored Procedures** ו\או **Parameterized Queries**.

11.3.5.4. יש לבצע בדיקות קלט לכל החלקים של בקשת ה – **HTTP: URI, Headers** ו – **Payload**. במיוחד אם שרת המערכת מבצע פעולה על-סמך ערכים אלו.

11.3.5.5. במידה ומתכנתים ב- **Java Script**, מעבר מידע מ – **DOM Context** אחד ל – **DOM Context** אחר יבוצע ע"י שימוש בפונקציות **JavaScript** מאובטחות, למשל: **innerText** או **val** (מניעת **DOM-based XSS**).

11.3.5.6. במידה וקיים שימוש ב – **Redirect** במערכת, יש לוודא לא מסתמכים על קלט המשתמש לביצוע ה – **Redirect** (מניעת **Open Redirect**).

11.4. בדיקות פלט

11.4.1.1. יש לוודא כי סיסמאות המשתמשים לא נשלחות חזרה למשתמשים.

11.4.1.2. יש לוודא כי לא נשלח מידע תפעולי למשתמשים (סוגי מערכות, שרתים, מערכות הפעלה בשימוש, אפליקציות וכדומה).

11.4.1.3. יש לוודא כי מבקשי מידע במשרדי הממשלה יקבלו את המידע המיועד עליהם, על בסיס ההזדהות ולמנוע העברת מידע אחר.

11.4.1.4. יש לבצע **Output Encoding** ו – **Sanitization** למידע שנשלח חזרה למשתמש שמקורו הוא ממידע שמוזן ע"י גורם אנושי.

11.5. הסרת מידע רגיש בעת הודעות שגיאה

11.5.1. יש לוודא כי בכל תקלה או שאילתה לא מועבר מידע רגיש או מידע תפעולי (על מערכות הספק, תשתיות וסוגי אפליקציה) החושף את מערכות המחשוב, השרתים והאפליקציות לסיכון או לניצול מתקפה ממוקדת.

11.5.2. הספק יוודא כי בעת הודעות כשל צד לקוח (דוגמת 400,401,403,404,410,413 ואחרים) וכן שגיאות מצד שרת (דוגמת 500,503,504 ואחרים), תופיע למשתמש הקצה הניגש לאתר, הודאת שגיאה כללית אשר תנוסח על ידי הספק אשר בעקבותיה יידרש הפונה לאתר לפנות טלפונית למוקד התמיכה של הספק.

11.6. ניהול שגיאות ריצה

אחד השלבים הראשונים של פורץ בהתקפת מערכת הוא שלב איסוף המידע. באמצעות איסוף מידע פנימי על המערכת, חולשות אבטחת מידע וסיכונים אפשריים בפגיעה ביציבותה, ינסה הפורץ לבצע ניסיונות ניצול של אלה לצורך גרימת שגיאות בלתי צפויות למערכת.

11.6.1. הנחיות לניהול שגיאות ריצה

11.6.1.1. יש לוודא כי המערכת אינה שולחת הודעות שגיאה או **Stack Traces** למשתמשי הקצה.

11.6.1.2. יש לשלוח הודעות גנריות בלבד ואת שגיאות הריצה לרשום ללוג בצורה מסודרת.

11.6.1.3. יש לוודא כי שגיאות הריצה נרשמות ללוג (כחלק מתשתית הלוגים של המערכת) בצורה מסודרת ומכילות את כל המידע הנדרש לחקירת השגיאה.

11.6.1.4. יש לוודא כי במידה וחלה שגיאת ריצה במערכת, הפעולה תיכשל ולא תעבור בהצלחה.

11.6.1.5. יש לוודא כי ה – **Developer Exception Page** אינו מופעל ב – **Production**. יש להגדיר דף שגיאות גנרי.

11.7. סריאליזציה ודה-סריאליזציה

11.7.1. בשנים האחרונות נמצאו מספר בפרצות בתהליכי ה-"סריאליזציה" **(Serialization)** וה-"דה-סריאליזציה" **(Deserialization)**.

11.7.2. הסיכון הזה הוא חלק מהסיכונים של **OWASP Top 10:2021**, ועל כן יש לבצע פעילויות-מנע בזמן הפיתוח כדי להימנע מקיום סיכון זה בקוד המפותח.

11.7.3. עדיף להשתמש בפורמט **XML** ו-**json** מאשר לבצע סריאליזציה (לפורמט בינארי) ודה-סריאליזציה (חזרה לפורמט המקורי).

11.7.4. יש לבצע סריאליזציה רק על אובייקט שיש לו חתימה-דיגיטלית, וזה כדי לוודא שלא מתבצעת מתקפה מסוג של "שינוי הנתונים" **(Data Tampering)** בין תהליך הסריאליזציה לבין תהליך הדה-סריאליזציה.

11.7.5. יש להשתמש בספריות עם גירסאות מעודכנות כדי להוריד את רמת הסיכון.

11.7.6. בשלב הדה-סריאליזציה, יש לוודא שבודקים היטב באיזה אובייקט מטפלים לפני שיוצרים אותו, תוך וידוא שמייצרים רק אובייקט מהסוג שמצפים שיהיה קיים בקלט.

11.7.7. יש להימנע מיצירת אובייקטים גדולים מדי אשר יכולים לגרום לתהליך של **DoS**.

11.7.8. יש לבצע את הדה-סריאליזציה בתהליך בעל הרשאות נמוכות ביותר.

11.8. גרסאות תוכנה והעלאה לייצור

11.8.1. בעת העלאה לייצור של קוד המערכת יש לוודא כי לא קיים מידע רגיש **Hardcoded** וש – **debug** מוגדר ל – **false**.

11.8.2. כל חלקי הקוד שאינם בשימוש ולא קיים בהם צורך - יימחקו.
11.8.3. קבצי קוד לא יימצאו בסביבת הייצור.
11.8.4. קבצי **Javascript, css, fonts** וכו' יישמרו בשרת המערכת. במידה ולא ניתן אלא להסתמך על מקור חיצוני, יש להטמיע שימוש ב **SRI** ו- **CSP**.
11.8.5. רכיבי התוכנה יהיו מעודכנים.
11.8.6. יש לנהל רשימה של רכיבי התוכנה \ חלקי קוד שבשימוש.

12. הגנה בתהליכי הזדהות אפליקטיביים ומסדי נתונים

12.1. הגנה בתהליכי הזדהות וניהול ה- **Session** - סיסמאות
12.1.1. יש לבצע שימוש במדיניות סיסמאות חזקה ומורכבת.
12.1.2. יש למנוע שמירת סיסמאות כ- **Clear Text**.
12.1.3. יש למנוע העברת סיסמאות כ- **Clear Text** (לדוגמא בפרוטוקול שאינו מוצפן).
12.1.4. יש לוודא שמירת סיסמאות באמצעים פונקציית **Hash** קריפטוגרפית חזקה – לדוגמה: **bcrypt**, **Argon2** או **pbkdf2**.
12.1.5. יש למנוע שליחת פרטי הזדהות (סיסמאות משתמשים) חזרה לדפדפן.
12.1.6. יש למנוע שליחת הודעות שגיאה המכילות פרטי זיהוי.
12.2. הגנה בתהליכי הזדהות וניהול ה- **Session** - פרוטוקולים
12.2.1. יש לבצע שימוש בפרוטוקולי הצפנה מסוג **TLS** גירסה1.2 ואילך. פרוטוקולים אלה מאפשרים שימוש באלגוריתמים חזקים ומאובטחים.
12.2.2. יש לציין באתר את הדפדפנים הנתמכים בגישה לאתר. זאת במטרה לאפשר למבקשי מידע במשרדי הממשלה לזהות כשל הנובע משימוש בדפדפן ישן שאינו תומך בפרוטוקולי הצפנה אלה.
12.3. הגנה על מידע בממשקים אפליקטיביים
12.3.1. יש למנוע שליחת הודעות שגיאה המכילות פרטים על מערכות, אפליקציות, רכיבי רשת, כתובות **IP**, ערכים פנימיים (מידע טכני).
12.4. תעודות אבטחה
12.4.1. רכישת תעודות אבטחה לאתר לזיהוי האתר יעשה מספק תעודות מוכר.
12.4.2. ניהול תעודות אבטחה למערכות פנימיות שאינן חשופות לאינטרנט באמצעות שרת **CA** פנימי.

13. הגנה על מידע רגיש בבסיסי נתונים

13.1. שמירת **Secrets**
13.1.1. יש לוודא כי לא נשמרות סיסמאות **Secrets** או מפתחות כ – **Hardcoded** בקוד המערכת.
13.1.2. יש לשמור נתונים רגישים (למשל – **connection string**) בקובץ קונפיגורציה (לדוגמה בקובץ **web.config**) בצורה מוצפנת.
13.2. הגנה על קבצי קונפיגורציה
13.2.1. קבצי קונפיגורציה מכילים הגדרות שונות על המערכת וכן מספר פרטי הזדהות לרכיבים אחרים המערכת.
13.2.2. יש להגביל את הרשאות הגישה לקבצי הקונפיגורציה למשתמש האפליקטיבי בלבד. הרשאות הגישה יהיו לקריאה בלבד (עפ"י הצורך העסקי).
13.2.3. יש להצפין כל מידע רגיש הנשמר בקבצי הקונפיגורציה: פרטי הזדהות ו – **Connection Strings**.
13.3. הצפנת מידע

13.3.1. מידע שיידרש בהצפנה וישמר בשרתי ה- **Data Base** יוצפן באמצעות מנגנון ההצפנה המובנה (לדוגמה) במערכת **BigQuery** באמצעות אלגוריתם הצפנה **AES**.

13.3.2. מפתח ההצפנה להצפנת המידע יישמר בצורה מאובטחת בשרת **KMS**.

13.3.3. הצפנה ופיענוח המידע יתבצע ע"י **Service** ייעודי בעל גישה לשרת המאחסן את המפתח.

14. הקשחת פרוטוקולים

14.1. הקשחת פרוטוקול **HTTPS**

להלן הנחיות אבטחה להקשחת פרוטוקול האפליקציה HTTPS המאפשר גישה של מבקשי מידע במשרדי הממשלה לאתר, לצורך קבלת מידע:

14.2. **HTTPS-Requests**

14.2.1. יש לעשות שימוש בבקשות – **POST** ולהימנע מבקשות **GET** ככל הניתן.

14.2.2. אין לשלוח מידע ממשתמשי הקצה לשרתי המערכת כפרמטרים ב – **URL**.

14.2.3. יש להגדיר רשימת **Whitelist** של ה – **HTTP-Methods** המותרים: **POST, HEAD, GET** ו – **PUT**.

14.2.4. יש לחסום כל **HTTP-Method** בלתי מורשה: **OPTIONS, DELETE, TRACE/TRACK, DEBUG** וכל **HTTP-Method** אחר.

14.3. **HTTPS-Responses**

14.3.1. יש לעשות שימוש ב – **HTTP Response Code**.

14.3.2. יש לשים דגש על שליחת ה – **HTTP Response Codes** הבאים:

14.3.2.1. **Bad Request** – 400: במקרה של בקשה במבנה לא תקין.

14.3.2.2. **Forbidden** – 403: במקרה של בקשה לא מורשית.

14.3.2.3. **Method Not Allowed** – 405: במקרה של שימוש ב – **HTTP-Method** לא מורשה.

14.4. **HTTPS Headers**

יש לעשות שימוש ב – HTTP Headers הבאים:

14.4.1. **Content-Type**:

14.4.2. לדוגמה עבור החזרת דף **HTML**

Content-Type: text/html

14.4.3. **HTTP Strict Transport Security (HSTS)**:

Strict-Transport-Security: max-age=31536000; includeSubDomains

14.4.4. **X-Frame-Options**:

X-Frame-Options: deny

14.4.5. **X-XSS-Protection**:

X-XSS-Protection: 1; mode=block

14.4.6. **X-Content-Type-Options**:

X-Content-Type-Options: nosniff

14.4.7. **Cache-Control** ואחרים (כאשר משתמשים ב-**Cookies**):

Cache-Control: no-cache, no-store, must-revalidate, max-age=0, s-maxage=0
Expires: 0
Pragma: no-cache

14.5. **TLS Cipher Suite**

14.5.1. יש לאכוף שימוש ב – **TLS v1.2** ואילך, ולמנוע שימוש ב – **TLS v1.1** ומטה.

14.5.2. יש לאכוף שימוש ב – **Ciphers** חזקים.
14.5.3. יש לאכוף שימוש במפתחות ארוכים: **256bit** עבור אלגוריתמי הצפנה סימטריים ו- **2048bit** עבור אלגוריתמי הצפנה אסימטריים.
14.5.4. יש לעשות שימוש בהגדרות והאלגוריתמים הבאים:
14.5.4.1. **SSLHonorCipherOrder On**.
14.5.4.2. **DHE**.
14.5.4.3. **RSA-Keys**.
14.5.4.4. **GCM – AEAD (Authenticated Encryption with Associated Data)**.
14.5.4.5. **SHA2**.
14.6. ניהול ה- **Session**
14.6.1. מיד לאחר סיום תהליך ההזדהות מול האתר, מתחיל תהליך ה - **Session** של האזרח המבקש את המידע. ה - **Session**. משמש כדי לעקוב אחר פעולות מבקשי מידע בשלבים השונים של מילוי הבקשה למידע.
14.6.2. יצירת ה- **Session**
14.6.2.1. לאחר זיהוי מבקש המידע יש לייצר עבורו **Session ID** באמצעות מנגנון מובנה ב - **Net**. המשמש ליצירת **Session ID**.
14.6.2.2. את ה – **Session ID** יש להעביר למשתמש באמצעות **Cookie** שיחזיק את ה – **Session ID** כ – **Value**.
14.6.2.3. ה – **Cookie** צריך להיות מוגדר עם הערכים **HttpOnly, Secure** ו- **SameSite=Strict**.
14.6.3. וידוא ה- **Session**
14.6.3.1. יש לוודא את תקינות ה – **Cookie** ואת תקינות ה – **Session ID** טרם ביצוע פעולות נוספות בצד השרת.
14.6.3.2. יש לבצע זאת עבור כל בקשה שנשלחת אל שרת המערכת.
14.6.4. מחיקת ה- **Session**
14.6.4.1. ה – **Cookie** וה – **Session ID** יהיו תקפים למשך שעה אחת בלבד (עפ"י הצורך העסקי – זמן מספק למילוי הפרטי הבקשה לרישום מבקש המידע).
14.6.4.2. יש להגדיר **Session Timeout** של 60 דקות שלאחריהם יהיה צורך בזיהוי מחודש.
14.6.4.3. יש להגדיר מנגנון **Logout** ולאפשר למשתמש לבצע יציאה מסודרת מהמערכת. מנגנון ה – **Logout** ייבצע מחיקה במערכת ל – **Session** של המשתמש וכן ישלח הודעת מחיקת המידע לדפדפן של מחשב המשתמש.
14.7. אכיפת הרשאות גישה
14.7.1. לאחר זיהוי מבקש המידע ויצירת **Cookie** על ידי המערכת, יש לשייך לו הרשאות לפעולות אשר הוא מורשה לבצע, למשל – מילוי פרטי הבקשה לקבלת מידע. להלן מספר עקרונות בנושא הרשאות, מידור ובקרת גישה אשר יש לפעול לפיהן:
14.7.1.1. יש לוודא כי טרם ביצוע פעולה במערכת, ייבדקו הרשאות המשתמשים – כלומר שמבקשי המידע כותבים או קוראים מידע הרלוונטי אליהם בלבד.
14.7.1.2. אין להסתמך על קלט מהמשתמש בעת ביצוע תהליך אכיפת ההרשאות. יש לעשות שימוש ב – **Session ID** כפי שמופיע ב – **Context** של שולח הבקשה.
14.7.1.3. יש לוודא שעקרון ה – **Least Privilege** מתקיים וכי משתמשי המערכת מורשים לגשת רק למידע, לפונקציות, לקבצים, **URLs**, שירותים ולכל משאב אחר, אשר אליו הם רשאים לגשת.

14.7.1.4. יש לוודא כי הערכים שעל פיהם מתבצעות החלטות ה – **Access Control** לא ניתנות לשינוי או מניפולציה ע"י משתמשי הקצה. יש לממש מנגנון זה ע"י בדיקות קלטים ולא ולהסתמך עליהם בעת החלטת אכיפת הרשאות, אלא להסתמך על מודל ההרשאות שנשמר בבסיס הנתונים של המערכת.

14.7.1.5. יש לוודא כי מנגנון ההרשאות במערכת הוא מרכזי ושכל החלטות למשאבים מוגנים מתבצעים דרכו.

14.7.1.6. יש לוודא כי החלטות של מנגנון ה – **Access Control** נרשמות ללוג, גם פעולות שנכשלו. את הלוגים יש לשמור במיקום מרכזי כפי שמתואר בפרק הלוגים.

14.7.1.7. יש ליישם מנגנון **Anti-CSRF** – בו יונפק **Token** לכל בקשת משתמש.

15. אבטחת ממשקים אפליקטיביים

15.1. כללי

15.1.1. כל חלק קוד \ רכיבי תוכנה צד שלישי יהיו ממקורות מהימנים בלבד אשר עברו בדיקות אבטחת מידע והלבנה.

15.1.2. יש לבצע את הפיתוח בתשתית מאובטחת ומתעדכנת.

15.1.3. לאחר רישום משתמש או אימות זיהוי מחדש של משתמש חוזר, יוצג למשתמש פרטי המשתמש, מועד הכניסה האחרון (אם בוצע), וכן שעון ותאריך עדכניים של מועד הכניסה העדכניים.

16. שימוש ב- WAF/XMLFW

16.1. הנחיות ליישום מערכת הגנה אפליקטיבית (**XMLFW/WAF**)

16.1.1. הספק יפעיל מערכת הגנה מפני מתקפות אפליקטיביות (דוגמת מערכת ה- **F5**).

16.1.2. המערכת תמוקם באופן אשר יאפשר לה לנטר את כל הרשתות האפליקטיביות והגישה לבסיסי המידע ותגן עליהם מפני איומים בשכבת האפליקציה ובין היתר סוגי המתקפות אשר פורטו במסמך זה בדגש על בדיקות קלט.

16.1.3. יש לוודא יכולות **Load Balance** להתמודדות עם מתקפות עומס ומתקפות אפליקטיביות.

16.1.4. יש לאפשר ניטור תעבורה מוצפנת, למשל באמצעות פתיחת ההצפנה על ידי מערכת אבטחת מידע, בדיקת התוכן, הצפנת המידע מחדש והעברתו ליעד.

17. שימוש ב- API Gateway

17.1. הנחיות ליישום מערכת **API gateway**

17.1.1. בפרוטוקולי **HTTP/S** ובכל ממשק **API** בו **Client** (או מספר **Clients**) פונים ליותר מ-ממשק **API** יחיד (**Many to Many / One to many**). נדרש הספק להטמיע פתרון **API Gateway** בין ממשקי **Client** לבין שירותי **API** פנימיים בפלטפורמה בכדי לחשוף מינימום ממשקי **API** ישירים בין ה- **Client** לבין מערכות הליבה.

17.1.2. יישום **API gateway** מול **Clients** חיצוניים (מחוץ לפלטפורמה) ידרשו מעבר מקדים של **WAF** ורק לאחריהן יוכלו לגשת לממשק ה- **API Gateway** במטרה לצמצם מתקפות אפליקטיביות על ממשקי ה- **API**.

18. אבטחת שירותי REST API

פרק זה מיועד לאבטחת שירות API .

18.1. תווך התקשורת

18.1.1. יש לאבטח את תווך התקשורת בין צרכני השירות לבין שרתי המערכת שחושפים את שירותי ה – **API**.

18.1.2. יש לאכוף שימוש בפרוטוקול התקשרות **HTTPs** בכל ה – **Endpoints** החשופים לרשת האינטרנט.

18.1.3. יש לעשות שימוש ב – **TLS v1.2**.

18.2. הזדהות

18.2.1. יש לבצע זיהוי של צרכני השירות באמצעות שימוש ב – **Mutual Authentication**, ע"י שימוש בשתי תעודות – אחת עבור שרת המערכת (חושף השירות) ושנייה עבור צרכן השירות (יש לייצר תעודה עבור כל צרכן שירות).

18.3. אכיפת הרשאות גישה

18.3.1. יש לעשות שימוש ב – **Attribute : [Authorize]**, לפני כל **End Point** שחשוף לצרכני השירות.

18.3.2. יש לזהות את צורך השירות (הספק) ולוודא כי הוא ניגש למשאבים החשופים עבורו בלבד.

18.4. שימוש ב – **HTTP Methods**

18.4.1. יש לאפשר שימוש במתודות הנחוצות בלבד ולאסור שימוש בשאר המתודות.

18.4.2. עבור כל בקשה אסורה יש לענות ב – **HTTP Response** עם הקוד – **405 Method Not Allowed**.

18.4.3. עבור כל בקשה שלא עברה בהצלחה את תהליך הזיהוי יש לענות ב - **HTTP Response** עם הקוד 401 – **Unauthorized**.

18.4.4. עבור כל בקשה למשאב אסור יש לענות ב – **HTTP Response** עם הקוד **403** – **Forbidden**.

18.5. שימוש ב – **HTTP Headers**

18.5.1. יש לעשות שימוש ב – **HTTP Headers** הבאים :

18.5.1.1. **Content-Type**.

18.5.1.2. **X-Content-Type-Options: nosniff**.

18.5.1.3. **X-Frame-Options: deny**.

18.5.1.4. **X-XSS-Protection: 1; mode=block**.

18.5.1.5. **Strict-transport-security: max-age**.

18.5.1.6. **Content-Security-Policy: frame-ancestors 'none'**.

18.5.1.7. **Cache-Control: no-store**

18.5.2. בנוסף, יש למנוע שימוש ב – **CORS** במידה ואפשרי ולא נעשה שימוש בקריאות **Cross-Domain**.

18.6. בדיקות קלטים ופלטים

18.6.1. יש ליישם את הבדיקות הבאות :

18.6.1.1. בדיקות אורך – מינימום ומקסימום.

18.6.1.2. בדיקות טווח.

18.6.1.3. סוג הקלט.

18.6.1.4. פורמט הקלט.

18.6.2. יש לאסור כל שימוש שלא במבנה שהוגדר כתקין.

18.6.3. מומלץ להגדיר את מבנה ה - **Input (Request)** וגם את מבנה ה - **Output (Response)** ולבצע וולידציה עפ"י המבנה שהוגדר.

18.6.4. יש ליישם את בדיקות הקלטים עם הגדרת **JSON Schema** עבור מבנה הקלט עבור כל שירות.

18.6.5. יש ליישם **JSON Schema** עבור הפלט שנשלח עבור כל שירות.

18.7. ניהול ה - **API**

18.7.1. יש למנוע גישה מרשת האינטרנט לכל **End-Point** שחושף ממשק ניהול.

18.8. ניהול שגיאות

18.8.1. יש לשלוח הודעות שגיאה גנריות בלבד לצרכני השירות. אין לחשוף מידע רגיש אודות טכנולוגיות המערכת ומידע טכני כזה או אחר לצרכני השירות.

18.8.2. במידה והתרחשה שגיאה יש לשלוח **HTTP Response** עם **HTTP Response Code** מתאים.

19. הנחיות להקשחת שירותי PUB/SUB

19.1. כללי

19.1.1. ממשקי **Pub/Sub** נועדו לניהול הודעות **RealTime** בין אפליקציות עצמאיות. הודעות אלה חשופות לסיכוני בעיקר לסיכוני אמינות וסודיות (התערבות בשדר). לפיכך שידור הודעות **Pub/Sub** יתבצע רק בממשקים מאובטחים דוגמת **HTTPS** ו- **Rest API** כאמור לעיל.

19.1.2. יש להצפין את השדרים.

19.2. הזדהות בתהליכי **Pub/Sub**

19.2.1. יש להגדיר הזדהות בשדרים (**Enable Authentication**).

19.2.2. ניהול ההרשאות יתבצע במערכת ה- **IAM** באמצעות חשבון **Service Account** ו- **Role** (**pubsub.publisher , pubsub.subscriber**) ייעודי לכל תהליך שידור או חשבון.

19.2.3. אין לעשות שימוש בחשבון גנרי.

19.2.4. יש לצמצם את ההרשאות בהתאם לעקרון ההרשאה המינימלי הדרוש.

19.2.5. יש לבצע בדיקות ולידציה וחתימתם באמצעות שירותי **GCP** ו- **OpenID Connect**

19.3. שימוש ב- **Token**

19.3.1. יש לוודא בדיקות אימות **JWT Token** (**Validate Token**) באמצעות הכנסת **Token** בכותרת בקשות. כל שרק שירותים מזוהים יקבלו שירות.

19.4. הגבלת ממשקים

19.4.1. יש להגביל את מקורות שבאפשרותם לשלוח הודעות לפי צורך עסקי או תפעולי ולהימנע מפתיחה רחבה.

19.5. ניטור

19.5.1. יש להפעיל **Audit Log** מלא על כל פעילות המתבצעת בשירות **Pub/Sub**.

19.5.2. יש לנטר ולהתריע על כשלים בהזדהות / **not authorized** ו- **Permission Denied**.

20. הנחיות אבטחת-מידע לשימוש בקוד פתוח (Open Source)

פרק זה רלוונטי לתהליכי פיתוח מבוססי Open Source וכן בשימוש בתהליכי Automation ובדיקות אוטומטיות (CI/CD) של ניהול רכיבי הפלטפורמה והרצת קוד.

20.1. כללי

20.1.1. בשנים האחרונות החלה עלייה בשימוש בקוד פתוח (**Open Source**) במערכות מחשוב בארץ ובעולם (דוגמת **Python , Ruby ,Go, Node.js, App Engine** ואחרים).

20.1.2. לצד היתרונות הרבים הגלומים בשימוש בקוד פתוח, דוגמת קיצור זמן פיתוח ועלויות, ישנה חשיבות לוודא כי הקוד הפתוח אינו יוצר פערים אבטחתיים.

20.1.3. יש לממש בקרות להפחתת איומי אבטחת-מידע בכל תהליך ה-**CI/CD** (**Continuous Integration / Continuous Deployment**), החל משימוש ב-**Source Repository** (כגון: **GitHub** או שרות ה-**Google Source Repositories** של **GCP** וכו'.) ועד ההתקנה האוטומטית כחלק מתהליך ה-**CD**.

20.2. אישור שימוש בקוד פתוח וחבילות תוכנה

20.2.1. הספק יעביר לראש תחום הגנת הסייבר של המזמין את כל חבילות התוכנה הצפויות לשימוש במסגרת הפעילות לצורך בדיקת סיכוני סייבר. לא יאושר שימוש בחבילות תוכנה אשר יכללו סיכונים מובנים או עלולים לאפשר תשתית ליישום סיכון או תרחיש אבטחה. לראש תחום הגנת הסייבר הזכות הבלעדית לאשר או למנוע שימוש בחבילות תוכנה.

20.2.2. הספק יעביר לתחום הגנת הסייבר במזמין את כל חבילות התוכנה הצפויות לשימוש במסגרת הפעילות לצורך בדיקת אופן ההרשאה לשימוש ברישוי במערכות **Open Source** לגופים ציבוריים (**EULA**, הסכמי רישוי למשתמשי קצה). הספק יישא בכל עלות ככל שתידרש במידה ורישוי ה-**Opensource** יגדיר זאת (רישוי בתשלום עבור גופים עסקיים, שאינם פרט). למזמין הזכות הבלעדית לאשר או למנוע שימוש בחבילות תוכנה אשר יגבילו את השימוש שלהם במסגרת מגבלות הרישוי.

20.3. הקשחת תהליך השימוש ב-**Source Repository**

20.3.1. יש לממש בקרות אבטחת-מידע כדי להפחית את איומי התוקפים. להלן הבקרות המומלצות:

20.3.1.1. יש לוודא הזדהות חזקה בכל גישה **Login** ל-**Source Repository**. זה כדי לאמת את זהות המשתמש באופן חזק יותר.

20.3.1.2. יש להגדיר שלפני כל ביצוע **commit**, יתבצע **review** של ראש הצוות או לפחות של מתכנת נוסף מטעם הספק. זה כדי למנוע מצב בו תוקף יצליח לעקוף את ההגנות ולבצע **commit** לקוד מסוכן (**malware**).

20.3.1.3. אחרי כל **commit**, יש לדרוש **approval** מחדש, גם לקטעי קוד שכבר בוצע להם בעבר תהליך של **commit** ו-**approval**. וכן עבור **commit** שתיקן תיקונים פשוטים כגון הערות או תיקון שגיאות כתיב. זה כדי למנוע מתוקף לנצל מצבים כגון אלה על-מנת להחדיר קוד עוין.

20.3.1.4. יש לחתום (**sign**) כל **commit** כדי שכולם יהיו יותר בטוחים לגבי הזהות של מי שביצע את ה-**commit**.

20.3.1.5. אין לאפשר קיום של חשבון **BOT** שמבצע שינויים ללא צורך של **review**.

20.3.1.6. יש להגביל גישה ל-**Source Repository** שלא אושרו על ידי המזמין.

20.3.1.7. יש לבטל שמות משתמשים שלא נעשה בהם שימוש הרבה זמן.

20.3.1.8. יש להגביל את כמות משתמשי ה-**admin**.

20.3.1.9. יש לבצע **Audit** על כל תהליכי העבודה מול ה-**Source Repository**, ולהעביר את קובץ ה-**Audit Log** באופן רציף למערכת **SIEM** אשר תדע לנתח אותו ולהתריע על ניסיונות תקיפה.

20.4. הקשחת תהליך בניית גרסה – **CI – Continuous Integration**

20.4.1. כחלק מתהליך בניית גרסה, יש להריץ כלי אנליזה סטטי מסוג של **SCA** (**Software Component Analysis**) שיבדוק באיזה ספריות קוד פתוח (**Open Source**) משתמשים ובמיוחד באיזה גרסה. זה כדי למנוע שימוש בקוד פתוח המכיל פרצות אבטחת-מידע או בקוד פתוח מזויף שהוכן על-ידי תוקפים.

20.4.2. יש להשתמש בכלי תוכנה שמייצר קובץ **SBOM** (**Software Bill Of Material**), שמכיל מידע על כל רכיבי התוכנה שבונים את המערכת, ובמיוחד את חלקי הקוד הפתוח בה משתמשת המערכת.

20.4.3. יש לשמור על ה-**secrets** שבהם משתמשים בתהליכי ה-**CI**. ה-**secrets** מאפשרים כניסה לרכיבי תוכנה. להלן מספר דוגמאות ל-**secrets**:

- API Keys – **בהם משתמשים לגשת לשירות חיצוני או ל-**API
- DB Credentials – **בהם משתמשים לגשת למאגר נתונים** (Database).
- SSH Keys – **בהם משתמשים לאשר זיהוי בגישה לשרתים מרוחקים**
- Git Credentials – **בהם משתמשים לגישה ל-**Source Repository

20.4.4. יש להצפין את ה-**secrets** ולא לשמור אותם גלויים כ-**Clear Text**.

20.4.5. יש לשמור את ה-**secrets** במקום מאובטח, כגון ב-**password manager** או בתיקיות שמורות היטב. אין לשמור אותם ב-**Source Repository**.

20.4.6. יש להשתמש ב-**secrets** שונים לצרכים שונים. לדוגמא: להשתמש בסיסמאות שונות בגישה ל-**databases** שנמצאים בפיתוח, בבדיקות ו/או בייצור.

20.4.7. להחליף (**rotate**) את ה-**secrets** בזמנים קבועים וקצרים (כל חודש או כל רבעון).

20.4.8. אין לכתוב את ה-**secrets** כ-**hard coded** בקוד. יש להשתמש רק בשם שלהם, ואילו את הערך, יש לשמור מחוץ לסביבת ה-**CI**.

20.4.9. יש להגביל את העברת ה-**secrets** לצעדי ה-**CI** (**CI steps**) למינימום הנדרש.

20.4.10. יש להגדיר את צעדי ה-**CI** (**CI steps**) עם רמת הפריווילגיה הנמוכה ביותר האפשרית.

20.4.11. לאפשר רק ל-**admin** לשנות את תהליך בניית הגרסה, ולא למתכנתים.

20.4.12. יש לבדוק את קבצי הקונפיגורציה של תהליכי ה-**CI/CD** באופן קבוע ולהגן עליהם מפני שינויים בלתי מאושרים.

20.4.13. יש לבצע **Audit** על כל תהליכי העבודה במהלך כל שלבי ה-**CI/CD**, ולהעביר את קובץ ה-**Audit Log** באופן רציף למערכת **SIEM** אשר תדע לנתח אותו ולהתריע על ניסיונות תקיפה.

נספח א' – תבנית מיפוי תהליכים והערכת סיכונים לדוגמה

מס'	נושא נבדק/תהליך אב	תאור התהליך/תת תהליך (בן)	אחראי על התהליך	מעביר המידע (מקור, מערכת מקור, רשת/סביבת מקור)	מקבל המידע (יעד, מערכת יעד, רשת/סביבת יעד)	אופן העברה	מערכות מעורבות בתהליך/מקום אחסון המידע	סיווג המידע (נוהל סיווג מידע)	תדירות העברת המידע (ממוצעת)	בחר סוג התווך מוצפן כן/לא	בחר רמת חשיבות לקיום תקין של התהליך בפרויקט
1	שם תהליך האב	תיאור תת התהליך 1	ספק	מערכת X	מערכת Y	ממשק API	מערכת X מערכת Y שרת אחסון	מידע חסוי רגיש/מידע תפעולי	תמידית (Online)	כן	**גבוהה מאוד**
2	שם תהליך האב	תיאור תת התהליך 2	מחלקה	עובד X	ספק	גלישה באמצעות דפדפן	שרת אפליקציה	מידע חסוי רגיש/מידע תפעולי	יומית	כן	**גבוהה מאוד**

הערות:

לאחר מיפוי התהליכים על ידי הספק, ובמסגרת ניהול הסיכונים המבוצע במזמין, יתווספו לטבלה עמודות נוספות לתיאור סיכונים בנושאי זמינות, סודיות, אמינות ובקרות מונעות, מגלות, אפקטיביות יישום הבקרות ופעולות נדרשות להפחתת הסיכונים.