נספח 2.0 - דרישות אבטחת מידע עבור ספק שירותי מחשוב ענן

עבור מכרז שיפור אמינות גיליונות הציונים והתעודות

מחב"א – מרכז החישובים הבינאוניברסיטאי

תוכן עניינים

[1. מבוא 3](#_Toc148448431)

[2. דרישות כלליות 3](#_Toc148448432)

[3. עמידה בתקני אבטחת מידע 5](#_Toc148448433)

[4. תשתית הענן 5](#_Toc148448434)

[5. אופן פיתוח המערכת 5](#_Toc148448435)

[6. תפעול המערכת 6](#_Toc148448436)

[7. ממשק הניהול של המערכת 6](#_Toc148448437)

[8. בקרת גישה 7](#_Toc148448438)

[9. העברת ושמירת מידע 8](#_Toc148448439)

[10. ניטור ובקרה 8](#_Toc148448440)

[11. ניהול אירועי אבטחת מידע 9](#_Toc148448441)

[12. גיבוי ושרידות 9](#_Toc148448442)

[13. בדיקות חדירות 10](#_Toc148448443)

[14. שמירה על סודיות ופרטיות 10](#_Toc148448444)

[15. שימוש, אחזקה וניהול מאגרי מידע 11](#_Toc148448445)

1. מבוא
   1. מחב"א (להלן: "המזמינה"), עושה שימוש במערך טכנולוגיות מידע לצורך ניהול ותפעול הפעילות העסקית שלה לרבות שימוש במערכות מידע, תשתיות מחשוב וכיו"ב.
   2. מחב"א מאוגדת כעמותה וחברות בה תשע האוניברסיטאות שלהלן: טכניון, אוניברסיטת חיפה, אוניברסיטה הפתוחה, אוניברסיטה העברית, אוניברסיטת בר-אילן, מכון ויצמן למדע, אוניברסיטת תל-אביב, אוניברסיטת אריאל ואוניברסיטת בן גוריון. בנוסף מחב"א תיתן שירות לאוניברסיטאות נוספות ולמכללות שיבחרו להצטרף למכרז זה. כלל המוסדות שיצטרפו לפרויקט (להלן: "מוסדות").
   3. בהמשך מחב"א תשקול בחיוב צירוף של גופים נוספים המעוניינים לבדוק אמינות תעודות אך אינם מעלים תעודות למאגר כמו גופי ממשל למשל (להלן: "מוסדות נוספים").
   4. התקשרות מחב"א עם הזוכה במכרז תעשה עבורה, ועבור המוסדות והמוסדות הנוספים.
   5. בהמשך מחב"א תשקול בחיוב צירוף של גופים נוספים המעוניינים לבדוק אמינות תעודות אך אינם מעלים תעודות למאגר כמו גופי ממשל למשל (להלן: "מוסדות נוספים").
   6. במסגרת הפעילות העסקית ולצורך קבלת שירותים שונים, המזמינה מתקשרת עם ספקים שונים בתחומים שונים ובין היתר, ספקי מחשוב ובפרט ספקי מחשוב ענן.
   7. ההתקשרות מול ספקי מחשוב ענן יכולה להתבצע בתצורות השונות (IaaS / PaaS / SaaS).
   8. מסמך זה נועד להגדיר דרישות אבטחת מידע בעת התקשרות עם ספק מחשוב ענן והמסמך תקף לכלל תצורות השירות (בהתאם לרלוונטיות של הפעילות).
   9. דרישות אבטחת מידע אלו מהוות חלק בלתי נפרד מהסכם ההתקשרות ומכילות הנחיות בהיבטי אבטחת מידע וזאת על מנת לשמור על סודיות, שלמות וזמינות המידע המנוהל ו/או המאוחסן אצל ספק מחשוב הענן (להלן: "**הספק**").
2. דרישות כלליות
   1. ספק המערכת בענן ימנה גורם אשר יהיה בעל אמון להיבטי אבטחת מידע במערכת ובכלל בתהליך ההתקשרות מול המזמינה. גורם זה יהיה אחראי על הטיפול במאגרי המידע המצויים בידי הספק וכן על יישום ההנחיות המופיעות במסמך זה.
   2. הספק יחתום מול המזמינה על הצהרה לשמירת סודיות בנוסף לנספח זה, בכל מקרה הספק מצהיר בזאת שלא יעביר מידע על מאגר זה ו\או הנתונים המצויים בו לכל גורם שהוא ללא אישור מוקדם ובכתב ממחב"א. הספק יודע שהפרת חובת סודיות זו מהווה הפרה יסודית וחמורה ביותר בהתקשרות שלו מול מחב"א.
   3. כלל עובדי הספק יעברו תהליכי גיוס על פי סטנדרטים מקובלים ולכל הפחות יעברו מבדקי מהימנות. עובדי הספק יוחתמו על הסכם סודיות מול הספק.
   4. כלל רכיבי המערכת יאוחסנו ויתופעלו על גבי תשתיות הממוקמות בתחומי מדינת ישראל ו/או מחוץ למדינת ישראל, במדינות המותרות על פי הרשות להגנת הפרטיות להעברת מידע על פי חוק ותקנות הגנת הפרטיות.
   5. הספק מתחייב כי המערכת המוצעת תעמוד בכל דרישות חוק הגנת הפרטיות ותקנותיו בהיבטים של שמירת מידע רגיש על פי חוק הגנת הפרטיות כפי שמתפרסמים מעת לעת על ידי משרד המשפטים במדריך המלא לתקנות אבטחת הפרטיות (אבטחת מידע). ראו גרסה אחרונה [כאן](https://www.gov.il/BlobFolder/guide/data_security_guide/he/המדריך%20המלא%20ליישום%20תקנות%20אבטחת%20מידע%20–PDF%20להדפסה_1.pdf).
   6. למען הסר ספק, עקרונות האבטחה המצוינים במסמך זה יחולו על כל חלקי המערכת ושרתיה כולל שרתי פיתוח, בדיקות וייצור, ממשקים חיצוניים ותת מערכות הנגזרות ממנה, בין אם מסופקים על ידי הספק או ספקי שירות לספק המערכת.
   7. המערכת תיישם, בכל השכבות, עקרונות של הפרדה מלאה בין מערכות הפיתוח והבדיקה למערכת הייצור, על מנת למנוע פגיעה אפשרית במערכת הייצור, עקב שינויים במערכות הפיתוח או הבדיקה. נדרש כי יהיו סביבות ממודרות ומופרדות האחת מהשנייה ומחולקות בתצורה הבאה:

סביבת פיתוח

סביבת בדיקות

סביבת ייצור

כך שלכל סביבה יהיו הרשאות וניהול נפרדים

ובסביבות הנמוכות (פיתוח בדיקות ) לא יישמר מידע אישי רגיש.

* 1. הספק מודע לכך שצרכי אבטחת המידע משתנים מעת לעת ושמחב"א רשאית לדרוש ממנו עדכונים בנושא, הספק מתחייב לבצע עדכונים אלו בלו"ז סביר ומהיר כפי שיוגדר על ידי מחב"א.

1. עמידה בתקני אבטחת מידע
   1. ספק השירות, יהיה בעל הסמכה בתוקף באחד או יותר מתקני אבטחת המידע הבאים:

ISO/IEC 27001

STAR level 2

ISO/IEC 27017

AICPA SOC 2/3

1. תשתית הענן
   1. Single Tenant – הקצאת תשתית וירטואלית ייעודית עבור המזמינה. במידה ולא ניתן ליישם "ענן פרטי", המערכת תותקן על גבי תשתית משותפת (Multi-Tenant) כאשר רכיבי המזמינה יהיו ייעודיים עבור המזמינה ולא ניתן יהיה להגיע לרכיבים השייכים לאוניברסיטה מרכיבים אחרים שנמצאים בתשתית המשותפת.
   2. מנגנוני הגנה על גבי תשתית הענן:

התקנת WAF (Web Application Firewall) בהתאם לסטנדרטים מקובלים.

קיום של Firewall כולל בקרה על חוקי FW.

קיום של מערכת IPS לניטור תעבורה בזמן אמת.

קיום מערכת לניטור וחסימת מתקפות סייבר (DDOS, בדיקות אנומליה ברשת וכו').

* 1. דרישות מספק השירות מחוץ לגבולות מדינת ישראל למידע מוגן וחסוי
     1. בשלב זה תאושר העברת מידע רק למדינות החברות באיחוד האירופי.
     2. על הספק להיות בעל תקן ISO 27001 תקף של השירות בענן או תקן מקביל בנושא ניהול אבטחת מידע.
     3. על הספק לפרט אם השירות בענן עומד בתקני אבטחת מידע בין-לאומיים (כדוגמת זה של Cloud Security Alliance).
     4. על הספק לבצע מידור של התשתיות הלוגיות (כגון שרתים לוגים, מסדי הנתונים ושירותים נוספים) משירותים של לקוחות אחרים המשתמשים בשרותי ענן. יש לפרט את ארכיטקטורת הרשת התומכת בתקן זה.
     5. על הספק לפרט את התכנית לניהול אבטחת המידע של השירות בענן.
     6. על הספק לפרט את תדירות ביצוע בדיקות חוסן באופן עצמאי וגם על ידי מומחה חיצוני בשכבות התקשורת, מערכת ההפעלה והאפליקציה של השירות בענן.
     7. על הספק לפרט את תדירות ביצוע של סקרי אבטחת מידע באופן עצמאי וגם על ידי מומחה חיצוני בשכבות התקשורת, מערכת ההפעלה והאפליקציה של השירות בענן.
     8. הספק מתחייב כי שימוש בכלים ו/או בשירותים משלימים ו/או חיצוניים לענן יעמדו בדרישות המפורטות במסמך זה.
     9. כל התקשורת לניהול סביבת הענן תתבצע על גבי תווך מוצפן עם הזדהות חזקה.
     10. על ספק שירותי ענן להעביר הודעה מראש לספק על הפסקת שירות – אם ספק הענן נאלץ להפסיק את השירות כתוצאה מצו בית משפט, הפרה של חוק/תקנות או בשל החלטה עסקית/פיננסית.
     11. על ספק שירותי ענן לאפשר העברת המידע והנתונים לספק טרם הפסקת השבתת השירות.

1. אופן פיתוח המערכת
   1. הספק מתחייב כי המערכת תפותח על פי סטנדרטים מקובלים של פיתוח מאובטח (SSDLC) ובהתאם לדרישות המזמינה.
   2. הספק מתחייב כי כלל עובדי הפיתוח ועובדים רלוונטיים נוספים, ככל שיהיו, יעברו הכשרה ייעודית לפיתוח מאובטח. הספק ידווח אודות תוכן ההדרכה והמשתתפים בה.
   3. הספק מתחייב כי יבצע בדיקות קוד תקופתיות (Code Review) על מנת לוודא כי קוד המערכת נקי מנוזקות.
   4. הספק מתחייב לאפשר למחב"א (כנציגה של המוסדות) לבצע סקרי אבטחת מידע ו/או מבדקי חדירה מבוקרים על מנת לבחון את אופן יישום היבטי אבטחת המידע במערכת. הספק מתחייב לתקן את הליקויים ברמה קריטית וגבוהה ככל שיהיו בפרק זמן אשר יוגדר עם המזמינה.
2. תפעול המערכת
   1. הקשחות שרתים

הספק יבצע הקשחות לכלל רכיבי המערכת על בסיס שיטות עבודה מקובלות ומומלצות, למוסדות שמורה הזכות להעביר הנחיות הקשחה נוספות לפי הצורך.

המערכת לא תכלול שמות משתמשים גנריים כגון: Admin, DBA כיו"ב.

* + 1. כל שליפת מידע ועדכון נתונים ייבדקו למניעת פגיעה בשרתי מסדי הנתונים, בנתונים ולמניעת פגיעה בנתונים.
    2. על הקבלן ליישם מערכת Database Firewall להגנה על מסדי הנתונים של המערכת.
    3. על מנת לנתר ולהגן על הנתונים שרתי היישום ימוקמו מאחורי חומות אש אפליקטיבי
    4. השרתים ימוקמו מאחורי מערך חומות אש ו IPS למניעת התקפות על היישום.
    5. השרתים יוקשחו לפי הגדרות היצרן כולל מערך בקרה
    6. תצורת הפתרון תכלול מערך זמינות על מנת להבטיח גישה רציפה ליישום
    7. העלאת הקבצים לאתר דרך היישום תתבצע תוך כדי בדיקת הקבצים מפני וירוסים ונוזקות והלבנתם (באמצעות מערכת ICAPאו פתרון אחר
    8. על הקבלן להקשיח את היישומים הן לפי הנחיות היצרנים והן למתן מענה בפני ניצול חולשות היישומים ו\או ניצול יכולות המערכת שלא הוגדרו כהלכה,

לדוגמא: אי החלפת סיסמת ברירת המחדל של מנהל המערכת.

* 1. סריקות ועדכוני אבטחה

הספק יבצע סריקות תקופתיות בהתאם לתקנות אבטחת הפרטיות (אבטחת מידע) של הרשות להגנת הפרטיות במשרד המשפטים, לצורך איתור פגיעויות וחולשות ברכיבי המערכת על פי הנדרש בחוק ויבצע עדכונים בהתאם לנדרש.

הספק יבצע עדכוני אבטחה למערכת על בסיס תקופתי (אחת לרבעון לכל הפחות). עדכוני אבטחה קריטיים יותקנו במידי עם קבלת העדכון.

הפצת העדכון תתבצע לאחר גיבוי המערכת ולאחר וידוא רציפות תפקודית של המערכת.

* 1. ניהול שינויים

הספק יתחזק נוהל ניהול שינויים (תשתיתיים ואפליקטיביים), כאשר הספק יעדכן את המזמינה על כל שינוי מהותי שיבוצע במערכת (לדוגמה: שינוי בארכיטקטורת המערכת, שינוי באופן פיתוח המערכת, שינוי במנגנון ההזדהות ו/או ההרשאות של המערכת וכיו"ב).

* 1. הפרדת סביבות

סביבת הייצור של המערכת תופרד לוגית באופן מלא מסביבות הפיתוח והבדיקות של המערכת וזאת על מנת לצמצם את הסיכון לפגיעה אפשרית במערכת בעקבות שינויים במערכות הפיתוח ו/או הבדיקות.

העברת גרסה לסביבת הייצור תבוצע באופן מבוקר ולאחר וידוא כי לא ייגרם נזק לסביבת הייצור ו/או פגיעה ברציפות התפקודית.

לא יועבר מידע של המוסדות לסביבות אחרות שאינן ייצור ללא אישור מפורש ובכתב ממנהל אגף המחשוב ומערכות המידע של המוסדות או הממונים על ידם.

תבוצע הפרדה של המידע לאזורים שונים לפי מוסד, כך שפריצה למידע של מוסד אחד לא יאפשר גישה למידע של מוסד אחר.

1. ממשק הניהול של המערכת
   1. הגישה לממשק הניהול של המערכת יוגבל לרשימת מורשים בלבד כאשר רשימה זו תצומצם למינימום הנדרש.
   2. הגישה לממשק הניהול תתאפשר מטווח כתובות IP מוגדר מראש.
   3. עובדי הספק הנדרשים לגשת לממשק הניהול יוגבלו למינימום הנדרש וככל הניתן לא תינתן להם גישה לנתונים של המוסדות.
   4. הזדהות לממשק הניהול תתבצע באמצעות אימות על ידי שני גורמי אימות (Two Factor Authentication).
2. בקרת גישה
   1. זיהוי ואימות

המערכת תכלול מנגנון זיהוי ואימות, ולא תאפשר כניסה ללא אימות המשתמש.

המערכת תאפשר סינון ומניעת גישה על בסיס מיקום וכתובות IP.

ככל הניתן, המערכת תאפשר התממשקות למערכת ניהול משתמשים של האוניברסיטה לטובת ניהול משתמשים וקבוצות הרשאה. לכל הפחות, המערכת תאפשר ניהול משתמשים מקומי לרבות מנגנון זיהוי ואימות.

מנגנון הזיהוי והאימות של המערכת יכלול הענקת משתמש אישי לכל משתמש במערכת ולא יותר שימוש במשתמש גנרי לעובדים. שימוש במשתמש גנרי יתאפשר למשתמשים אפליקטיביים בלבד וחריגה מכך תאושר על ידי מנהל אבטחת המידע של המוסדות.

במקרה של כישלון בהזדהות, המערכת תציג הודעת שגיאה גנרית, ללא חשיפה של פרטים אודות השגיאה.

יוגדר במערכת פרק זמן קבוע שלאחריו יופעל מנגנון ניתוק תקשורת המחייב זיהוי ואימות מחדש של המשתמש בכל הדפים. הניתוק יבוצע על ידי סיום תוקף של הSession בצד השרת ולא על ידי העברת הלקוח לדף הכניסה.

* 1. ניהול משתמשים והרשאות

המערכת תכלול מנגנון הרשאות על ידי יצירת פרופילים שונים והענקת הרשאות ספציפיות (עד לרמת השדה הבודד) לכל פרופיל בהתאם לתפקיד ו/או לפי הצורך.

הענקת ההרשאות תהיה פרטנית לפי משתמשים ו/או לפי קבוצות משתמשים.

המשתמשים במערכת ינוהלו על ידי המוסדות

המערכת תבצע ולידציה על ההרשאות שניתנו למשתמש בהתאם לפרופיל שהוגדר.

* 1. ניהול סיסמאות

המערכת תאפשר ניהול סיסמאות על פי הסטנדרטים של המוסדות.

המערכת תאפשר הזדהות באמצעות אימות על ידי שני גורמי אימות (Two Factor Authentication).

סיסמאות המנוהלות במערכת הסיסמאות יגובבו באמצעות פונקציית גיבוב (HASH) מאובטחת כגון SHA-2  ומעלה ולא יישמרו באופן גלוי, לא בתווך התקשורת ולא בבסיס הנתונים.

המערכת תאפשר נעילה ושחרור של משתמשים בהתאם למדיניות המוסדות.

המערכת תאכוף החלפת סיסמה ראשונית (אשר התקבלה בעקבות פתיחת חשבון חדש על ידי מנהל מערכת) ו/או לאחר שחרור מנעילה.

1. העברת ושמירת מידע
   1. מידע רגיש על פי חוק הגנת הפרטיות יישמר באופן מוצפן בבסיס הנתונים של המערכת על ידי שימוש בטכניקות הצפנה מקובלות ושימוש בסטנדרט הצפנה של AES-256 לכל הפחות.
   2. תווך התקשורת אל מול תשתית הענן יהיה מאובטח בפרוטוקול מוצפן (לדוגמה: TLS 1.2).
   3. מפתחות ההצפנה ו/או תעודות דיגיטליות רלוונטיות ינוהלו על ידי ספק הענן ויישמרו באופן מאובטח.
   4. ההצפנה של המידע תהיה אישית המפתחות יועברו לסטודנטים ולא ישמרו במערכת בשום צורה.
   5. יעשה שימוש ב-REST API או SOAP API. יעשה שימוש בכלים לאבטחת הפרוטוקול כמו API Gateway, ושימוש בתשתיות OAuth 2.0 לצרכי הזדהות של ה-API.
2. ניטור ובקרה
   1. המערכת, תאפשר קיום לוג אירועים, אשר ניתן יהיה לניטור ולתחקור.
   2. לוג האירועים יישמר במסד הנתונים של האפליקציה וניתן יהיה לקרוא אותו במידת הצורך. כמו כן ניתן יהיה לייצא לוג זה (בעדיפות לקבציי אקסל) לטובת ניטור ותחקור בזמן אמת.
   3. לוג האירועים יתנהל בשתי רמות:

רמת ניהול המערכת – לוג זה מיועד לכלול את האירועים המבוצעים ברמת ניהול האפליקציה ועל ידי משתמשים המוגדרים "מנהלי מערכת".

רמת השימוש במערכת – לוג זה מיועד לכלול את האירועים המבוצעים על ידי משתמשי הקצה.

* 1. מדיניות הלוגים תכלול לפחות את המרכיבים הבאים, עבור כל סוגי המשתמשים במערכת:

10.4.1 מקור הפעולה: שם משתמש, כתובת IP

10.4.2 זמן הפעולה: תאריך ושעה

10.4.3 מידע אודות פעולות במערכת: כניסה, יציאה, ניסיון התחברות, עדכון שדה, מחיקה וכיו"ב

10.4.4 פרטי השינוי לרבות ערך ישן וערך חדש יוצגו בלוג רק כאשר המערכת במצב חקירה זמני כמתואר בסעיף 10.4.7

10.4.5 מערכת הלוגים במצב יצור לא תכיל מידע אישי רגיש כפי שמוגדר בחוק (שילוב של השם המלא עם אחד מהבאים - יוגדר כמידע רגיש: מספר תעודת זהות, כתובת דואר אלקטרונית, מידע על צנעת, חייו האישיים של אדם, לרבות התנהגותו ברשות היחיד, מידע רפואי או מידע על מצבו הנפשי של אדם, מידע גנטי כהגדרתו בחוק מידע גנטי, התשס"א-2000, חברות באיגודים מקצועיים, מידע אודות דעותיו הפוליטיות או אמונותיו הדתיות של אדם, מידע על אודות עברו הפלילי של אדם, נתוני מיקום, מידע ביומטרי, מידע על נכסיו של אדם, חובותיו והתחייבויותיו הכלכליות, מצבו הכלכלי או שינוי בו, יכולתו לעמוד בהתחייבויותיו הכלכלית ומידת עמידתו בהם, הרגלי צריכה של אדם שיש בהם כדי ללמד על מידע לפי פרטים או על אישיותו של אדם, אמונתו או דעותיו.)

10.4.6 מערכת הלוגים לא תכיל מידע שמאפשר להגיע למידע רגיש כמו הקוד שמאפשר שליפה של המידע אודות הסטודנט, מפתחות הצפנה ועוד.

10.4.7 מערכת הלוגים תכיל מידע רק לגבי ביצוע הפעולות

10.4.8 ניתן יהיה להעביר לוגים למצב זמני של חקירה בו ישמרו פרטים מלאים לזמן קצוב של לא יותר מ-36 שעות. לאחר 36 שעות המערכת תחזור באופן אוטומטי למצב שבו נתונים אינם מוצגים בלוג, והמידע המפורט ימחק באופן אוטומטי

1. ניהול אירועי אבטחת מידע
   1. הספק יישם מנגנוני ניטור ובקרה לצורך זיהוי אירועי אבטחת מידע במערכת.
   2. הספק יגדיר נוהל לטיפול באירועי אבטחת מידע אשר יכלול את אופן ההתמודדות עם אירועי אבטחת מידע לרבות דיווח לגורמים רלוונטיים.
   3. הספק מתחייב לעדכן את המוסדות באופן מיידי בכל חשש של פגיעה במידע של המוסדות (לרבות דלף מידע, שיבוש נתונים ו/או השבתת נתונים).
   4. במקרה של אירוע ממשי, הספק מתחייב להעביר לידי המוסדות באופן מיידי תחקיר אירוע עם פרטי האירוע, השתלשלות האירועים והנזק שנגרם ו/או העלול להיגרם כתוצאה מהאירוע, ואף להפעיל צוות IR במידה ויידרש.
2. גיבוי ושרידות
   1. ארכיטקטורת המערכת תכלול כלים, שיטות ואמצעים לגיבוי נתונים ולהתאוששות מתקלות ונפילות מערכת אשר יעמדו בדרישות האלה לפחות:

ביצוע גיבויים שוטפים, לפחות אחת לארבע שעות, ושמירת לוגים והיסטוריית גיבויים, לשנה לפחות.

גיבוי שלא הסתיים בהצלחה, יופעל מחדש.

ביצוע תהליכי "צילום מצב" ושחזורים יהיה שקוף למשתמשים ולא יגרום להפרעה בפעילותם השוטפת.

הספק יבצע בדיקות שחזור מדגמיות באופן תקופתי, לפחות אחת לחודש.

קיום אתר גיבוי מרוחק לאתר המרכזי עם יכולת מעבר בין האתרים בתוך מספר שעות בהתאם לSLA שיוגדר בהסכם ההתקשרות מול הספק.

* 1. הספק ישתמש לצורך גיבוי ו- DR בכלים מובנים של ספק הענן אשר יכללו:

שרותי DR מנוהל להתאוששות מלאה של אפליקציות בענן ללא איבוד מידע

כלים המאפשרים המשכיות עסקית (RPO של שניות) בעלות נמוכה

הגנה מפני התקפות Ransomware על ידי חזרה לכל נקודת זמן

1. בדיקות חדירות
   1. בדיקת חדירות - הספק מתחייב לבצע בדיקות חדירות באמצעות חברה חיצונית בלתי תלויה המתמחה בבדיקות חדירות אפליקטיביות ותשתיתי למערכות המשמשות לאחסון, עיבוד והתשתיות התומכות במכרז זה. בדיקות אלה יבוצעו לפני העלאה לייצור ואחת לשנתיים כחלק מתהליך התחזוקה החברה שתבצע את בדיקת החדירות תיבחר ע"י מנהל אבטחת המידע של מחב"א בהסכמת מנהלי אבטחת של המוסדות האקדמיים.
   2. Code review – הספק מתחייב לבצע סריקת קוד דינאמי וסטטית, דוח יועבר לאנשי אבטחת מידע של המוסדות. התהליך יבוצע לפני העלאה לייצור וכן בעקבות פעילויות תחזוקה
   3. על הספק לתקן את הליקויים שהתגלו בבדיקת חדירות טרם עליית המערכת לייצור.
2. שמירה על סודיות ופרטיות
   1. הספק מתחייב לעמוד בהוראות חוק המחשבים, התשנ"ה 1995 – דיני הגנת הפרטיות ובכללם חוק הגנת הפרטיות, התשמ"א, 1981 ותקנות הגנת הפרטיות [)אבטחת מידע ( התשע"ז .2017](https://www.gov.il/he/Departments/General/data_security_info)
   2. הספק מתחייב למלא אחר כל הוראות אבטחת המידע לגבי שמירת מידע כפי שיועברו ע"י מחב”א והמוסדות.
   3. הספק ידאג לאבטחת כל חומר שיגיע אליו במסגרת ביצוע התחייבויותיו על פי הסכם זה ויהיה אחראי כלפי מחב”א והמוסדות על כל המידע המועבר אליו או דרכו לרבות דוחות, נתונים אישיים, תכתובות דוא"ל, קבצים, מסמכים, שרטוטים וכיו"ב על פי ההנחיות שיועברו על ידי מחב”א והמוסדות.
   4. באחריות הספק לדאוג לחיסיון, אמינות וזמינות המידע של מחב”א והמוסדות שברשותו.
   5. הספק יהיה אחראי לכל עקיפה או ניסיון עקיפת מנגנוני אבטחה ובקרות גישה לתשתיות שונות, שיבוצע על ידי מי מהעובדים מטעמו.
   6. בעת אירוע אבטחת מידע או אירוע חריג אצל הספק בו קיים חשד לגבי דלף מידע של מחב”א והמוסדות, הספק מחויב להודיע באופן מידי לאיש הקשר מטעם מחב”א והמוסדות.
   7. הספק מתחייב לשתף פעולה עם מחב”א והמוסדות בכל אירוע חריג בו מעורב עובד הספק, או שקיים חשד למעורבות שיש עמה השלכה ישירה או עקיפה על ביטחון מערכות המידע של מחב”א והמוסדות, בכל הפרה או חשד להפרה של חוקים תקנות או נהלי אבטחת מידע כולל בחקירת אירועים או חשדות לחריגות אבטחת מידע או דליפת מידע של מחב”א והמוסדות לגורמים בלתי מורשים.
   8. מידע רגיש של מחב"א והמוסדות יהיה נגיש לעובדי הספק ע"פ הגדרת הצורך לדעת Know) to (Need.
   9. הכנת עותקים לצרכי עבודה אצל הספק תיעשה על פי צורך בלבד ותפוצתם תהא
   10. בקרב עובדי הספק הנדרשים לעותקים אלו בלבד.
   11. חל איסור על הספק להעביר מידע לגורמי צד שלישי
   12. על הספק ליישם יכולת הגדרה במערכי הניטור לרישום גישה או ניסיונות גישה

למידע המוגדר כרגיש.

* 1. על הספק ליישם יכולת סימון של רמות רגישות המידע בדוחות המערכת.
  2. על הספק לדאוג לכך כי תיושם יכולת ערבול (Obfuscation) של נתונים המועברים

סביבת ה- production לסביבות אחרות.

* 1. הספק מתחייב להפריד הפרדה מלאה את מאגרי מחב"א והמוסדות המצויים בידיו מיתר מאגרי המידע שברשותו.
  2. בכל מקרה שבו לספק התקשרות עם צד שלישי כלשהו אשר יש לה נגיעה עם ההתקשרות בין הספק למחב”א ולמוסדות במסגרת מכרז זה ו/או על יישום ההנחיות המפורטות במסמך זה, הספק מתחייב להודיע על כך למחב"א ולמוסדות ולפעול על פי הנחיותיו וכן ליידע את הצד השלישי על החובות הנובעות מקיום ההנחיות המפורטות במסמך זה.
  3. הספק מתחייב לשתף פעולה עם נציגי מחב"א והמוסדות לצורך שמירה על אבטחת המידע והפרטיות.

1. שימוש, אחזקה וניהול מאגרי מידע
   1. כל המידע, התוכנות, האפליקציות, הנתונים, קוד וכו' אשר יאוחסנו על ידי הספק יהיו בבעלותו המלאה והבלעדית של מחב”א והמוסדות. הספק יצהיר כי הוא מוותר על זכותו לתבוע כל זכות קניינית ממחב”א והמוסדות ,ובכלל זה את הזכות לקניין רוחני. למען הסר ספק, כל החומר המועבר על ידי מחב”א והמוסדות לספק וכל המידע הנצבר במערכות אשר לספק גישה אליהם הינו בבעלות מחב”א והמוסדות כולל זכויות הקניין חומרי ורוחני והינם בבעלותו הבלעדית ואין לספק כל זכות לתבוע שימוש במידע או לבצע בו כל שימוש שאינו באישור מחב”א והמוסדות.
   2. כל שינוי במדיניות הספק בנוגע ליישום ההנחיות במסמך זה יובא לידיעת ואישור מחב”א .
   3. הספק מתחייב שכל גישה שלו, או של מי מטעמו, למידע ולמאגר המידע, תתבצע אך ורק בהתאם להוראות מחב”א והמוסדות ולמטרות אשר הוגדרו לו על ידי מחב”א והמוסדות במסגרת ההתקשרות.
   4. הספק מתחייב שהוא, או מי מטעמו, לא יעביר מידע, או חלק ממידע, מתוך מאגרי מחב”א והמוסדות אשר בידיו או שיש לו גישה אליהם, לצד שלישי כלשהו ללא אישור מפורש ובכתב מאת מחב”א המוסדות.
   5. הספק מתחייב למנוע שמירה של נתונים רגישים באופן מקומי אצל משתמשי המערכת. במקרים חריגים יש לקבל אישור מפורש ובכתב ממחב"א והמוסדות.

ולראייה באנו על החתום:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

שם חתימה וחותמת