

מדינת ישראל
משרד החינוך
המינהל למדע ולטכנולוגיה

דו"ח בדיקת אבטחת מידע בסביבה מתוקשבת

(גרסה 15.1, 16/01/2017)

א. פרטי הסביבה והבודק המקצועי

סביבה לבדיקה		בודק
שם הסביבה:	שם הבודק:	
שם היצרן:		
כתובת הסביבה:	סוג סביבה:	
שם איש קשר:	טלפון איש קשר:	
תאריך בדיקה פיזית:	תאריך ומספר בדיקה:	תאריך בדיקה: _____, בדיקה מספר: _____

ב. קישורים

תיאור	הקישור
תקן אבטחת מידע	http://sites.education.gov.il/cloud/home/meyda_le_sapakim/Documents/teken_avtahat_meyda.pdf
הנחיות לבדיקת חוסן אפליקטיבית	http://sites.education.gov.il/cloud/home/meyda_le_sapakim/Documents/bdikar_hosen.pdf
תקנים והנחיות טכנולוגיות כלליות עבור ספקים וגופים מפתחים	http://sites.education.gov.il/cloud/home/meyda_le_sapakim/Pages/tkani_m_veanhiot_tehnologiot_klaliot_avur_sapakim_vegufim_mefathim.aspx

ג. סיווג הסביבה והסעיפים לבדיקה

סיווג	תיאור המידע	סעיפים לבדיקה
בלמ"ס	מערכת שאינה שומרת ו/או מעבדת מידע ו/או נתונים על אישיותו של אדם, צנעת אישיותו, מצב בריאותו, מצבו הכלכלי, הכשרתו המקצועית, דעותיו ואמונתו וכדומה, לדוגמה: ת"ז, תמונה	סביבות אינטרנט סעיפים 31-45
מידע מוגן/רגיש	מערכת השומרת ו/או מעבדת נתונים ו/או מידע על אישיותו של אדם, צנעת אישיותו, מצב בריאותו, מצבו הכלכלי, הכשרתו המקצועית, דעותיו ואמונתו וכדומה, לדוגמה: ת"ז, תמונה, ציונים, משימות, דואר וכו'	כל הסעיפים למעט אלו שמסומנים כמידע חסוי
מידע חסוי	מידע שפגיעה בזמירותו, בשלמותו, באמינותו, בסודיותו או בשרידותו עלולה לגרום לתקלות כגון אלה: - פגיעה או הכבדה על ביצוע תכניות או פעולות כלכליות, מנהליות, חברתיות, משפטיות ואחרות של המדינה. - גרימת תקלה לעבודת הגופים הציבוריים שמשמעה עיכוב או ייקור תהליכי עבודה או הפרעה בביצוע אכיפת החוק. - מידע פנים ארגוני שהנהלת הארגון רוצה לשמור על חשאיותה מול ארגון מתחרה	כל הסעיפים

ד. סעיפים לבדיקה

תיאור הבדיקה	הערות הבודק	הערות/הצהרת יצרן (ימולא על ידי יצרן)	X/V
הכנסת נתונים			

מדינת ישראל
משרד החינוך
המינהל למדע ולטכנולוגיה

X/V	הערות/הצהרת יצרן (ימולא על ידי יצרן)	הערות הבודק	תיאור הבדיקה
			1. יש לוודא שהתוכנה בודקת כל נתון המגיע מהמשתמש, בטפסים, cookies, query HTTP headers, strings
			2. הבדיקות מתבצעות בצד השרת - אין לסמוך על בדיקות ב-client
			3. המערכת תבדוק את סוג הטקסט, אורכו, קידוד, טווח וכן תחפש מילות מפתח וסימנים אסורים
			4. יש לסנן ולקבל רק קלט שעבר בדיקה
			5. יש לתעד ולהזהיר במקרה של קלט לא חוקי
			6. אין להפנות לדף שגיאה בעת הזנת קלט לא חוקי, יש להציג הודעה ברורה למשתמש למשל: "שם משתמש או סיסמא אינם תקינים"
			טיפול במידע רגיש
			7. זיהוי וטיפול בנתונים רגישים: סיסמאות, פרטי התחברות לשרת ולבסיס נתונים, נתוני תלמידים אישיים, גישה למשאבים מחוץ למערכת
			8. אין לאגור נתונים סודיים לא חיוניים לתפקוד המערכת (כמו כרטיסי אשראי, מידע רפואי)
			9. במידה ונעשה שימוש באמצעות המערכת לגבייה או סליקת תשלום שיש לפעול בהתאם להוראות ודרישות רמ"ט הרשות למשפט, טכנולוגיה ומידע http://www.justice.gov.il/Units/ilita/LawInfo/Hanchayot/HanchayotBetokef/Pages/default.aspx
			10. אין להעביר מידע רגיש ב cookies כמו ת.ז, או ב- HTTP-GET
			הזדהות וסיסמאות
			11. הסיסמא לא תעבור גלויה ברשת אלה בצורה מוצפנת (SSL)
			12. המערכת תספק למשתמש את היכולת להחליף את הסיסמא בעצמו, בצורה בטוחה, בכל עת
			13. אורכם של שמות המשתמשים של במערכת יהיה לפחות 6 תווים ולא יהיה ת.ז. של תלמיד ולא ת.ז של הורה. שם משתמש יכול להיות דואר אלקטרוני
			14. סיסמת התלמיד והמורה לא תהיה קצרה מ 6 תווים וסיסמת המנהל לא תהיה קצרה מ-6 תווים, ותהיה מורכבת משילוב של ספרות ואותיות
			15. סיסמתו של מנהל המערכת (אדמיניסטרטור) תהיה באורך של 8 תווים לפחות וכוללת תווים ומספרים
			16. טרם החלפת הסיסמא על המשתמש יהיה להקליד את סיסמתו הנוכחית
			17. 5 ניסיונות שגויים לנעילת המשתמש, או לשלב CAPCHA לאחר 3 ניסיונות כושלים

מדינת ישראל
משרד החינוך
המינהל למדע ולטכנולוגיה

X/V	הערות/הצהרת יצרן (ימולא על ידי יצרן)	הערות הבודק	תיאור הבדיקה
			18. פרק זמן לספירת ניסיונות כושלים : 10 דקות
			19. הסיסמא הראשונית של המשתמש תהייה רנדומאלית ובהתאם למבנה שהוגדר לעיל
			20. המערכת תחייב את המשתמש להחליף את סיסמתו הראשונית בעת ההתחברות הראשונה למערכת
			21. אין להציג את הסיסמא למשתמש באף מסך במערכת
			22. אין לאפשר שמירת הסיסמא ב COOKIE יש לחסום את האופציה לשמירת הסיסמא באמצעות הדפדפן
			23. יצירת סיסמא חדשה במקרה בו המשתמש שכח את הנוכחית תהייה אך ורק לאחר זיהוי המשתמש באמצעים אחרים, כגון כתובת דואר אלקטרוני, SMS או שאלות סודיות וכדומה
			24. סיסמת המשתמש תשמר בצורת hash בבסיס המידע
			25. על המערכת לחסום שימוש בסיסמאות קודמות, שמירת היסטוריית סיסמאות, עד 3 סיסמאות אחורה
			26. אחת ל-6 חודשים יש לחייב החלפת הסיסמה למורים לאחר 6 חודשים, ולתלמידים לאחר שנה
			27. אם המערכת מיועדת לגני ילדים וכיתות א' ומטה: * חוזק סיסמה - 6 מספרים לא עוקבים, ביניהם לא יהיו 3 מספרים זהים ברצף. * מספר ניסיונות שגויים לנעילה - 7 ניסיונות או לשלב CAPCHA לאחר 4 ניסיונות כושלים; מומלץ CAPCHA המורכב ממספרים. * תדירות החלפת הסיסמה – אחת 24 חודשים
			28. גישה לנתונים בעלי רגישות גבוהה מתבצעת על ידי הזדהות נוספת מלבד שם משתמש וסיסמא
			29. במידה ושרתי הסביבה מתארחים בעננים ציבוריים מחוץ לגבולות ישראל , גישה אליהן ברמת הרשאה של מנהל מערכת (Admin) תתבצע באמצעות המנגנונים הבאים בלבד: 1. התחברות באמצעות הזדהות חזקה- שימוש במנגנון לייצור סיסמה חד פעמית (OTP) וברכיבי אחסון לסיסמאות (TOKEN) 2. התחברות באמצעות כלי מאובטח לגישה מרחוק, לדוגמא sslvpn, checkpoint וכו'
			הרשאות
			30. המערכת תגדיר מספר הרשאות (כגון משתמש, תלמיד, מורה, מנהל, אדמיניסטרטור וכו')
			31. בכל דף במערכת תתבצע בדיקה שרק בעל ההרשאות המתאים יכול לגשת אליו (פרט

מדינת ישראל
משרד החינוך
המינהל למדע ולטכנולוגיה

X/V	הערות/הצהרת יצרן (ימולא על ידי יצרן)	הערות הבודק	תיאור הבדיקה
			לדפים המוגדרים כ"חיצוניים" המורשים לכלל הגולשים
32.			הבדיקה תתבצע בצד השרת
			ניהול הגדרות
33.			המערכת (האפליקציה) תרוץ תחת חשבון עם רמת הרשאות הנמוכה ביותר הניתנת כך שלא תאפשר ביצוע פעולות לא רצויות ע"י משתמשים רגילים
34.			יש לבדוק גישה מאובטחת לניהול מרחוק, יש להתחבר לשרת באמצעות RDP או לוח בקרה אחר, רק באמצעות שם משתמש וסיסמא
35.			אין לשמור מידע על התחברות וסיסמאות בקובצי טקסט, או בקבצים לא מוגנים
			Session Management
36.			אין להעביר את נתוני הזיהוי של המשתמשים בין מחשב המשתמש לשרת המערכת, למעט דף הכניסה למערכת
37.			יש לקיים מנגנון Idle Timeout אשר יסיים את ה-Session של המשתמש לאחר מספר דקות מוגדר, כ-60 דקות, של חוסר פעילות במערכת
38.			יש לקיים מנגנון Session Timeout אשר יסיים את ה-Session לאחר זמן ארוך של פעילות במערכת, כ-10 שעות. מנגנון זה נועד למנוע שימוש במערכת באמצעות סקריפטים וכדומה
39.			יש לנתק את Session במצבי שגיאה אפליקטיביים, כך שאם המערכת נפלה לא יישאר SESSION פתוח אליו תלמיד אחר יכול להתחבר
40.			ניתוק ה-Session יבוצע על ידי סיום תוקף ה-Session בצד השרת, ולא על ידי העברת הלקוח לדף הכניסה בלבד
			עדכוני תוכנה
41.			יש לבדוק שבמערכת ההפעלה, databases, בשרת האינטרנט ובשאר התוכנות המשמשות את המערכת מותקנים עדכוני התוכנה האחרונים
			חדירות מערכת הפעלה
42.			בדוק אילו פורטים פתוחים, ודא שאין פורטים פתוחים ללא צורך
43.			וודא שהשירות המתאים מאזין לכל פורט פתוח
44.			שימוש רק בפרוטוקולים ובפורטים מוכרים
			הקשחה ושרידות
45.			האם מותקן אנטי וירוסים על השרת.
46.			האם קיים מערך חומת אש ורכיבי IPS למניעת התקפות על היישום
47.			תצורת השרתים תכלול מערך זמינות על מנת להבטיח גישה רציפה ליישום
48.			לא יופעלו שירותים ואפליקציות על שרתי היצור אשר אינם נחוצים לפעולה תקינה של המערכת

מדינת ישראל
משרד החינוך
המינהל למדע ולטכנולוגיה

X/V	הערות/הצהרת יצרן (ימולא על ידי יצרן)	הערות הבודק	תיאור הבדיקה
			תיעוד (logging) ואזהרות
49.			הפעלה של תיעוד מלא ואזהרות מערכת על פעולות לא מורשות
			שיתוף
50.			הימנעות משיתוף של מקומות לא הכרחיים, והגנה בסיסמה על שיתופים נחוצים
			מודרציה וניטור
51.			יש לאפשר למורה לנעול חשבונות תלמידים
52.			יש לאפשר למורה לשנות סיסמא של תלמיד
53.			המערכת תדאג לכך שכל תוכן שהועלה למערכת ע"י תלמיד יינטר ויבדק לפני הצגתו לשאר התלמידים במרחב. (הבדיקה תתבצע ע"י מורה או בעל תפקיד אחר) המערכת תאפשר למורים למחוק תכנים לא ראויים שהוזנו ע"י תלמידים גם לאחר פרסומם. 2 האופציות צריכות להתקיים בסביבה ועל בית הספר להחליט באיזה תצורה הוא מעוניין לעבוד
54.			יש להציג דוחות סטטיסטיים לגבי השימוש במערכת של תלמידים
			אישורים נלווים לבדיקה
55.			אישור בדיקות חדירות אפליקטיבית מחברה חיצונית
56.			אישור ביצוע סקר סיכונים
57.			אישור התקנת עדכונים שוטפים על שרת הייצור מהחברה המארחת את הסביבה
58.			אישור ופירוט לגבי האבטחה הפיזית של השרתים מהחברה המארחת את הסביבה
59.			אישור ביצוע בדיקת עומסים ותוצאות הבדיקה, כולל כלי הבדיקה
60.			(חסוי) יש להציג למשרד דוחות זמינות ועומסים בתשתיות וביישומים לא יותר מאחת לחודש, למעט במצב חירום או תרגיל
			דרישות מספק השירות מחוץ לגבולות מדינת ישראל למידע מוגן וחסוי
61.			האם הסביבה או הגיבוי של הנתונים מתארחים מחוץ לגבולות מדינת ישראל, במדינות החברות באיחוד האירופי?
62.		יש לספק אישור או הפניה לתקן	האם תצורת תשתית כשירות היא ברמת laas?
63.			היצרן נוקט אמצעים מספיקים להבטחת פרטיותם של משתמשי המערכת? ומבטיח שלא יועבר מידע לאף גורם זולתו בין אם באותה מדינה ובין אם במדינה אחרת
64.		יש לספק אישור או הפניה לתקן	האם ספק שירות האירוח עומד בתקן שירות בענן או תקן מקביל בנושא ניהול אבטחת מידע לדוגמה (ISO27001)
65.		יש לפרט את ארכיטקטורת הרשת	על היצרן לבצע מידור של התשתיות הלוגיות כגון שרתים לוגים, מסדי הנתונים ושירותים

מדינת ישראל
משרד החינוך
המינהל למדע ולטכנולוגיה

X/V	הערות/הצהרת יצרן (ימולא על ידי יצרן)	הערות הבודק	תיאור הבדיקה
			נוספים משירותים של לקוחות אחרים המשתמשים בשירותי ענן. יש לפרט את ארכיטקטורת הרשת התומכת בתקן זה
66.		יש לפרט את התכנית לניהול אבטחת המידע של השירות בענן	על היצרן לפרט את התכנית לניהול אבטחת המידע של השירות בענן
67.		יש לפרט את תדירות בדיקות חוסן	על הספק שירות האירוח בענן לפרט את תדירות ביצוע בדיקות חוסן באופן עצמאי וגם על ידי מומחה חיצוני בשכבות התקשורת, מערכת ההפעלה והאפליקציה של השירות בענן
68.			על ספק שירותי האירוח להעביר הודעה מראש ליצרן על הפסקת השירות, לדוגמה כתוצאה מצו בית משפט, הפרה של חוק/תקנות או בשל החלטה עסקית/פיננסית
69.			על ספק שירות האירוח לאפשר העברת המידע והנתונים לספק טרם הפסקת השבתת השירות
70.			האם הגיבוי מתבצע ביחד עם גיבויים של ספקים אחרים (במידה וכן יש להצפין את הגיבוי)
71.			הספק מתחייב שבכל פנייה למערכת ולרשומות במאגר יירשמו כל הנתונים הבאים: זהות המשתמש, כתובת IP, התאריך והשעה של ניסיון הגישה, רכיב המערכת שאליו בוצע ניסיון הגישה, סוג הגישה, היקפה, ואם הגישה אושרה או נדחתה
72.			(חיוני) הצהרה לגבי scalability במערכות, איזה ארכיטקטורה היצרן משתמש, מהו כלי איזון העומסים, ובתוך כמה זמן יכול היצרן לעמוד בהרחבה בעת הצורך. כמו כן הצהרת לגבי שרידות ויכולת הרחבה של Web, Database, Firewall, תקשורת ושרתים
73.			הצהרה על עמידה בלפחות 30% מהעומס בתקופות של פעילות רגילה של המערכת
			אפליקציות
74.			הצהרת יצרן שהיישום לא שומר מידע מוגן או חסוי במכשיר ללא הצפנת הנתונים
75.			היישום מאפשר למשתמשים למחוק את כל הנתונים הקשורים אליו באופן פשוט וברור
76.			היישום לא משתמש בזיכרון מטמון של מערכת ההפעלה לשמירת מידע מוגן/חסוי
77.			ניתן לאפשר הזדהות אוטומטית לזמן מוגבל של עד 10 דקות בלבד של חוסר פעילות, לאחר 10 דקות יש לדרוש הקלדת הסיסמא
78.			ההזדהות לאחר 10 דקות של חוסר פעילות או שלילת מידע חדש מהשרת, חייבת להתבצע מול שרת מרוחק ולא באופן מקומי על המכשיר
79.			לאחר 5 שעות זמן פעילות במערכת יבוצע ניתוק מהשרת ותידרש הקלדה נוספת לשימוש
80.			התקשורת בין היישום לשרת ההזדהות צריכה להיות מוצפנת ומאובטחת
81.			במידה והיישום עושה שימוש בנתונים השמורים במכשיר כגון: אנשי קשר, תמונות ופרטים אישיים של המשתמש יש לקבל אישור המשרד

מדינת ישראל
משרד החינוך
המינהל למדע ולטכנולוגיה

X/V	הערות/הצהרת יצרן (ימולא על ידי יצרן)	הערות הבודק	תיאור הבדיקה	
			ולחוסף הערה לכך במגבלות האישור	
			בכל שימוש של היישום בחיישנים או ברכיבים נוספים הקיימים במכשיר, היישום יידע את המשתמש ויבקש את אישורו	82.

ה. מסקנות

ו. סיכום תוצאות בדיקת אבטחת המידע:

עבר []

לא עבר []