קבלה, תמיכה ותחזוקה של מערכות ISO 27799		
	מהדורה	2.0
	בתוקף מ	ינואר 2018
	א.14.2	עמוד 1 מתוך 10

ניהול אישורים

תאריך	שם	תפקיד	חתימה
30/09/2012	שי אמיר	ממונה אבטחת מידע	שי
09/09/2015	שי אמיר	ממונה אבטחת מידע	שי
01/08/18	ראובן אליהו	ממונה אבטחת מידע	ראובן

ניהול שינויים

תאריך	מחבר	גרסא	מהות השינוי
1/3/07	רן אדלר	1.0	da
1/5/07	יהושע פסין	1.1	עריכה
16/2/08	יהושע פסין	1.2	שינוי שם מסמך ישים
9/8/09	מורנו נאור	1.3	מספור הנוהל בהתאם לתקן + הוספת סעיפים 5.6, 5.7.
19/02/2012	טליה זמיר יהושע פסין	1.4	התאמה לתקן ISO 27799
22/08/2012	טליה זמיר תמיר פלדמן	1.5	התאמה לתקן ISO 27799
17/11/2014	אורנסק	1.7	התאמות לדרישות תקן ISO 27001:2013 עדכון סעיף 5.7.1
09/09/2015	גבי פטליס	1.8	בקרה

01/01/2018	אורנסק	2.0	התאמה לתקן ISO 2016:27799

1. מטרה

1.1. הגדרת תהליך קבלת מערכות מידע חדשות לשימוש משרד הבריאות, תוך הקפדה על עמידה בדרישות אבטחת המידע ויישום תהליך תמיכה ותחזוקה מאובטח במערכות.

2. הגדרות

2.1. קלט/ פלט: תוצרי מערכת, תעבורת הנתונים במערכת.

3. מסמכים ישימים

3.1.1. נוהל א.14.2.1.1 - 'פיתוח מערכות מאובטחות'.

3.1.2. נוהל א.13.1 – 'אבטחת תשתיות'.

4. אחריות ליישום

4.1. מנהל מערכות מידע.

5. שיטה

5.1. תהליך פיתוח המערכת:

5.1.1. בכל דרישה לפיתוח / רכישה של מערכת מידע, ימלא המשתמש טופס בקשה ובו יסביר את דרישתו.

5.1.2. טופס הבקשה ייחתם ויאושר ע"י מנהל היחידה המבקשת ויועבר לממונה אבטחת מידע .

5.1.3. לכל מערכת מידע ימונה בעלים, באחריות בעלי מערכות מידע לקבוע את סיווג המערכת.

5.1.4. באחריות ממונה אבטחת מידע לקבוע את ההגנות הנדרשות ע"מ לשמור על רמה נאותה של אבטחת מידע בהתאם לרמת הסיווג של המערכת.

5.2. פיתוח תוכנה על ידי קבלני שירות - במידה ופיתוח התוכנה מתבצע ע"י חברת ספק, יש לשקול את הנושאים הבאים:

5.2.1. סידורי רישוי, הבעלות על הקוד, וזכויות קניין אינטלקטואלי.

5.2.2. אישור האיכות והדיוק של העבודה המתבצעת.

5.2.3. סידורי הפקדה למקרה כשל של צד שלישי כגון פשיטת רגל, אבדן הקוד וכו'.

5.2.4. זכויות גישה לבדיקת האיכות והדיוק של העבודה שנעשתה.

5.2.5. דרישות חוזיות לשילוב אבטחת מידע בקוד.

5.2.6. בדיקה לפני ההתקנה לגילוי קוד זדוני.

5.2.7. שימוש בתכנה אינו מצריך הרשאות מנהל (Administrator) בתחנה אלא של משתמש רגיל בלבד.

5.3. תכנון קיבולות - על כל מערכות המידע לעמוד בקיבולות הנדרשות לפעילותן התקינה. האחראים על הפיתוח והתפעול יקבעו את רמת הקיבולות הנדרשת. תכנון הקיבולות יכלול לפחות את הבאים:

5.3.1. גודל וניצולת של דיסקים.

5.3.2. תעבורת רשת.

5.3.3. חלוקת עומסים.

5.3.4. יכולת עיבוד נתונים.

5.3.5. דרישות זיכרון.

5.3.6. גדילה צפויה כתוצאה משימוש במערכת.

5.4. ניתוח וניסוח של דרישות אבטחה:

5.4.1. בקרות המשתלבות בשלב תכנון מערכת הינן זולות משמעותית ליישום ותחזוקה מִבַּקרות המוספות מאוחר יותר.

5.4.2. בשלב ניתוח וגיבוש הדרישות של פיתוח מערכות חדשות או שיפור מערכות קיימות, ממונה אבטחת מידע יהיה מעורב ויזוהו כל דרישות האבטחה, ינומקו, יוסכמו ויתועדו כחלק מתיק אפיון המערכת.

5.4.3. דרישות האבטחה יביאו בחשבון את הבקרות האוטומטיות אשר יש לשלב במערכת.

5.4.4. דרישות האבטחה ואמצעי הבקרה ישקפו את הסיווג של הנכסים המעורבים, ואת הנזק הצפוי במקרה של כשל אבטחה או העדר אבטחה ולכן יש לקבוע את הדרישות רק לאחר שלב סווג והערכת הנכס על ידי בעלי המידע של הנכסים המעורבים בהתאם לנוהל ניהול סיכונים.

5.4.5. הדרישות לאבטחת מידע בהם יש להתחשב מופיעים בנוהל א.13.1 – 'אבטחת תשתיות' בהיבט הפיתוח יש לפנות לנוהל א.14.2.1.1 - 'פיתוח מערכות מאובטחות'.

5.4.6. שלב הבדיקה יכיל בדרך כלל 3 סוגי בדיקות -

5.4.6.1. בדיקה הכוללת אישור איכות של המערכת עצמה ותקינות עיבוד הנתונים הפנימי.

5.4.6.2. בדיקה הכוללת בחינה של יחסי הגומלין והממשקים של המערכת עם מערכות אחרות.

5.4.6.3. בדיקה ברמת המשתמש הבוחנת את המערכת בהתאם לתרחישים המוגדרים על ידי המשתמש - בהתאם לדרישות מן המערכת.

5.4.7. הבדיקות לקבלת המערכת יבוצעו בהתאם לדרישות מוגדרות. על הבדיקות בנושא אבטחת מידע לכסות את הנושאים הבאים -

5.4.7.1. אפשרויות של ניהול משתמשים וסיסמאות.

5.4.7.2. מנגנוני בקרה ומעקב.

5.4.7.3. מנגנוני הרשאות ובקרת גישה.

5.4.7.4. מבחני קיבולת ועמידה בעומסים.

5.4.7.5. היבטי זמינות ועמידות נגד התקפות.

5.4.7.6. התאוששות מתקלות.

5.4.7.7. אפשרויות של מערכת גיבוי לנושאי המשכיות עסקית.

5.4.7.8. בדיקות חדירה ופריצה.

5.4.7.9. אבטחת קבצי המערכת וקוד המקור.

5.4.7.10. מנגנוני אימות נתונים.

5.4.7.11. בחינת תקלות ידועות מראש/חזויות.

5.4.7.12. השפעה על רמת האבטחה במערכות אחרות.

5.4.7.13. אינטגרציה עם מערכות אבטחה קיימות ומתוכננות (מערכות ניהול משתמשים וכו').

5.4.7.14. התאמה לסטנדרטים נפוצים.

5.4.7.15. התאמה לכל הדרישות והתרחישים.

5.4.7.16. קלות שימוש.

5.4.7.17. קלות ניהול.

5.4.8. תהליך הבדיקה יבוצע בסביבת בדיקה ייעודית המופרדת באופן לוגי מכל מערכת אחרת ואינה מכילה כל נתוני אמת.

5.4.9. במידה ויש צורך להעלות נתוני אמת יש לבצע ערבול הנתונים (scrambling) על כל מידע חסוי / חסוי ביותר או מידע המאפשר להגיע למידע חסוי.

5.4.10. לאחר בדיקת מערכת תוך שימוש בנתוני אמת או בנתונים מעורבלים, יש לבצע מחיקה של כל הנתונים טרם העלאת המערכת לאוויר.

5.4.11. יש להימנע ככל הניתן מהעלאת נתוני אמת ללא ערבול למערכות לשם בדיקתם. בכל מקרה של צורך להשתמש בנתוני אמת, יש לקבל אישור בכתב מממונה אבטחת מידע במשרד הבריאות.

5.4.12. מבחני האבטחה יבוצעו בשיתוף גורמי הסיסטם ו/או גורמים חיצוניים לפי החלטת ממונה אבטחת מידע.

5.5. הרשאות גישה:

5.5.1. הגישה לסביבת הפיתוח תותר למנהל הפרויקט, למנהל הפיתוח / מערכות מידע ולמפתחים בלבד.

5.5.2. מנהל פרויקט הינו הגורם היחיד אשר לו הרשאות להעלות שינויים לייצור.

5.5.3. במידת האפשר, הרשאות הגישה למפתחים תינתן בהתאם לשיוך פרוייקטלי. לכל פרויקט תוגדר סביבת עבודה ייחודית כך שגישת המפתח תתאפשר לפרויקטים אליהם הוא משויך בלבד.

5.5.4. במקרה של כשל בייצור, מפתחים יקבלו הרשאה נקודתית לגשת לסביבת הייצור לצורך בדיקת הכשל. הגישה לסביבת הייצור תבוטל מיד עם תום הטיפול בכשל. יש להימנע ככל האפשר מביצוע שינויים ישירות בסביבת הייצור גם במקרה של כשל.

5.5.5. סביבת הבדיקה (Test), תשמש את המפתחים והמשתמשים לצורך ביצוע בדיקות קבלה לפני מעבר לייצור.

5.6. הגבלות שינויים:

5.6.1. בעת מסירת תוכנות לביצוע שינויים הן אצל ספק חיצוני והן בתוך משרד הבריאות, תוצף דרישה לביצוע שינויים ברמה המינימאלית ביותר שתאפשר:

5.6.1.1. שדרוג התוכנה כנדרש להמשך תפקודה בצורה היעילה ביותר.

5.6.1.2. מניעת התנגשויות בין תוכנה בפיתוח לבין תוכנות או מערכות המוטמעות במשרד הבריאות.

5.7. עקרונות מנחים לביצוע בדיקות קבלה:

5.7.1. במהלך בדיקת ההטמעה של המערכת (Integration) יש לוודא כי אין למפתחים גישה למטרות עדכון וכי לא ניתן לבצע שינויים בקוד הנבדק ללא אישור.

5.7.2. אין להשתמש בהעתק של נתונים אמתיים מסביבת הייצור (Production).

5.7.3. יש לתעד את הליך הבדיקה כיאות.

5.7.4. בעת זיהוי בעיות במהלך הבדיקה, על המפתח לתעד את הבעיות, לבצע שינויים מתאימים בסביבת הפיתוח ולהגיש אותה לבדיקה חוזרת.

5.7.5. הבדיקה לשינוי בתוכנית ותוצאות הבדיקות.

5.8. מעבר מפיתוח לייצור:

5.8.1. באחריות מנהל הפרויקט לקבוע סט בדיקות QA ובדיקות אבטחה לביצוע לפני העברה לייצור, במסגרת הבדיקות ייבדקו רכיבי ומנגנוני אבטחת מידע שמופעלים במסגרת הפרויקט.

5.8.2. המעבר של מערכת מפיתוח לייצור יבוצע ע"י מנהל הפרויקט בלבד. למפתחים לא יינתנו הרשאות הנדרשות לטובת ביצוע המעבר.

5.8.3. כל התקנת מערכת בסביבת הייצור תיעשה בתאום ובאישור של מנהל מערכות מידע.

5.9. קליטת המערכת:

5.9.1. אין לאשר את המערכת לעבודה ללא אישור כי כלל המערכת עברה את כל מבחני אבטחת המידע ועונה על כל הדרישות בתחום זה.

5.9.2. כאשר המערכת החדשה משפיעה על מערכות אחרות, יש לקבל אישור מבעלי המערכות המושפעות טרם קבלת המערכת. זאת, לאחר הנחייתם באשר להשפעות הטכניות והתפעוליות הנוגעות להשפעה זו.

5.9.3. ועדת ההיגוי לנושאי אבטחת מידע תהיה מעורבת באישור קבלתן של מערכות מידע מרכזיות / קריטיות.

5.10. תמיכה ותחזוקת מערכות :

5.10.1. נוהלי בקרת שינויים, יבוצעו הפעולות הבאות -

5.10.1.1. מילוי טופס "טופס בקשה לקליטה/שינוי במערכת מידע" (נספח א') על ידי בעל מערכת המידע.

5.10.1.2. בעל מערכת המידע יגיש את הבקשה לשינוי למנהל הפרויקט, שיבדוק היתכנות השינוי.

5.10.1.3. במידה והשינוי בר ביצוע, מנהל הפרויקט יעביר את הבקשה למנהל הפיתוח ולממונה אבטחת מידע .

5.10.1.4. במקרה שהבקשה כרוכה בשינוי המשפיע על מערכת מידע אחרת, דרוש גם אישורו של בעל המידע באותה המערכת.

5.10.1.5. תבוצע סקירה של הבקרות הקיימות כדי להבטיח שהן לא יועמדו בסכנה על ידי השינויים.

5.10.1.6. זיהוי היישומים והתשתיות הדורשים שינוי בעקבות הבקשה לשינוי.

5.10.1.7. וידוא כי תיעוד המערכת מעודכן עם השלמתו של כל שינוי.

5.10.1.8. יבוצע ניהול גרסאות לכל עדכוני התוכנה.

5.10.1.9. תחזוקת נתיב ביקורת של כל הבקשות לשינוי.

5.10.1.10. וידוא כי תיעוד התפעול ונהלי המשתמש עודכנו במידת הצורך.

5.10.1.11. וידוא כי יישום השינוי מתבצע באופן הממזער הפרעות למהלך העבודה התקני במשרד הבריאות.

5.10.1.12. יש לבצע בדיקות אבטחת מידע לאחר השינויים.

5.10.2. דרישות שמירת התיעוד - מנהל מערכת המידע ישמור את כל טפסי בקשות השינוי.

5.10.3. התקנת תוכנה (deployment) - תוכנה חדשה או תוכנה אשר עברה שינויים חייבת להיבדק כיאות ולקבל אישור בהתאם לסטנדרטים של ניהול שינויים ובעיות טרם התקנתה בסביבת הייצור במשרד הבריאות.

5.11. בקרת גישה לספריית קוד מקור :

5.11.1. כדי להקטין את האפשרות להשחתת תוכניות מחשב, תקוים בקרה קפדנית על הגישה לספריות של תוכניות מקור.

5.11.2. יש לוודא כי רק הגורמים המורשים נגישים לספריות קוד המקור של המערכות.

5.11.3. תחזוקה והעתקה של ספריות תוכניות מקור, תיעשה תחת נהלים קפדניים של בקרת שינויים.

5.12. הגבלות שינויים לחבילות תוכנה :

5.12.1. רצוי להשתמש בתוכנות מדף מבלי לשנותו, כאשר נראה שיש צורך חיוני בשינוי בתוכנה כזו, יישקלו הנושאים הבאים -

5.12.1.1. הסיכון לבקרות הדיוק והשלמות המובנים.

5.12.1.2. קבלת הסכמה בכתב מבעלי התוכנה המאשרת את ביצוע השינוי.

5.12.1.3. האפשרות לקבל את השינויים הדרושים מבעלי התוכנה, כעדכון תוכנה תקני.

5.12.1.4. ההשלכות הנובעות מכך שמשרד הבריאות הופכת להיות האחראית להמשך התחזוקה, עקב השינויים שהוכנסו.

5.12.1.5. שינויים יבוצעו על עותק של התוכנה ולא על המקור, התוכנה המקורית תשמר.

5.12.1.6. כל השינויים ייבדקו בדיקה מלאה ויתועדו כך שניתן יהיה, בעת הצורך, ליישם אותם שוב פעם בעתיד.

5.12.1.7. יש לבדוק שאין פגיעה באבטחת המידע לאחר השינוי.

5.13. מבדקי חדירה :

5.13.1. במידת הצורך, ובהתאם לרמת סיווג המידע המאוחסן ונגיש למערכת, יתוכננו ויבוצעו מבדקי חוסן אפליקטיביים למערכות מידע עוד בטרם העברתם לייצור ע"פ אבני דרך שיוגדרו מראש במסגרת תהליך הפיתוח וההטמעה.

5.13.2. לשיקול דעתו של מנהל מערכות מידע לבצע בנוסף, מבדק חדירה תשתיתי בעת קבלת מערכת חדשה או שינוי מהותי במערכת קיימת.

5.13.3. לאחר ביצוע שינויים מהותיים במערכות המידע, יבוצע מבדק קבלה בהיבטי אבטחת מידע לפני העלאת המערכת המשודרגת לאוויר. המבדק יתבצע בשיטה של מבחן חדירה (Penetration Test) וייתן דגש על המודול בו בוצע השינוי והשפעתו על המערכת ומערכות מתממשקות.

5.14. הגנה על מידע באפליקציות הזמינות לציבור :

5.14.1. באפליקציות אירגוניות הזמניות לציבור יוטמעו מנגנוני אבטחת מידע ע"מ למנוע פגיעה בשלמות, זמינות ואמינות המידע המועבר בתהליך העברת המידע (Transaction).

5.14.2. לצורך כך יש לוודא יישום המנגנונים הבאים -

5.14.2.1. וידוא קיום תעודות אבטחה תקפה לאתר.

5.14.2.2. הזדהות מאובטחת למערכת ע"פ מדיניות בקרת הגישה של משרד הבריאות.

5.14.2.3. שמירת סודיות ואמינות המידע המועבר באמצעות :

5.14.2.3.1. הצפנת תווך העברת המידע.

5.14.2.3.2. שימוש בפרוטוקולים מוצפנים (HTTPS, FTPS וכו').

5.14.2.4. אחסון פרטי הטרנסאקציות המבוצעות יתבצע במקום שאינו נגיש לציבור/לרשת (ברשת משרד הבריאות בלבד).

נספח א': פורמט טופס בקשה לקליטה/שינוי במערכת מידע של משרד הבריאות

טופס בקשה לביצוע קליטה/שינוי במערכות המידע

פרטי העובד המבקש
שם העובד: _____ תפקיד: _____ מחלקה: _____
מהות השינוי
☐ שינוי במערכת קיימת ☐ מערכת חדשה שם המערכת: _____ מטרת השינוי והצורך המקצועי בשינוי/התקנה: _____ _____
הערכה אודות משאבי המחשוב הנחוצים
_____ _____
השפעה אפשרית על מערכות אחרות במשרד הבריאות ו/או תהליכים קליניים
_____ _____
השפעה אפשרית על משתמשי המערכת (כולל אבטחת מידע)
_____ _____
בדיקות נדרשות בטרם ביצוע השינוי (כולל אבטחת מידע)
_____ _____
המלצת מחלקת מערכות מידע לביצוע השינוי
פירוט משמעויות לביצוע השינוי/התקנה: _____ _____ שם העובד: _____ תאריך: _____ חתימה: _____
אישור בעל המידע
☐ שינוי / התקנה מאושרת ☐ שינוי / התקנה איננה מאושרת הערות / הנחיות לביצוע: _____ שם בעל המידע: _____ תפקיד: _____ חתימה: _____