

דרישות אבטחת מידע לספק מערכת לניהול ידע

- א. חברת "קנט קרן לנזקי טבע בחקלאות בע"מ" (להלן; "החברה") מעוניינת לרכוש מערכת לניהול ידע, מערכת מקומית, עצמאית אשר תרכז את המידע העסקי בתוך קנט.
- ב. להלן דרישות אבטחת המידע החלות על ספק התוכנה, הנובעות מהנחיות אבטחת המידע בדרישות החוק והאסדרה החלות על גופים מוסדיים (לפי חוק הגנת הפרטיות ותקנותיו, וחוזר גופים מוסדיים 2016-9-14)

1. דרישות כלליות

- 1.1. הספק מצהיר כי הוא פועל כנדרש על פי החוק, התקנות ותיקוני הגנת הפרטיות וכי הוא נוקט באמצעי אבטחה ובקרה כמתחייב מהוראות חוק הגנת הפרטיות, תיקוניו ותקנותיו והנחיות רשם מאגרי מידע.
- 1.2. הספק יחתום ויחתים את העובדים מטעמו הרשאים לגשת למידע, על הצהרת סודיות, הכוללת, בין היתר, התחייבות לשמירה מוחלטת על אבטחת המידע של החברה.
- 1.3. הסכם SLA.
- 1.4. הספק מתחייב לא להעביר לצד שלישי מידע שיתקבל במסגרת ההתקשרות, או להשתמש במידע שעובדיו יחשפו אליו אגב ביצוע ההתקשרות, לכל מטרה אחרת שלא קשורה לביצוע ההתקשרות.
- 1.5. הספק יוודא הפקדת קוד מקור בחברה או אצל נאמן.
- 1.6. החברה תוודא שקוד המקור עבר בדיקה נגד חשיפות ואי קיום קוד זדוני באמצעות סריקת חשיפות אבטחת מידע (Vulnerability Scan).
- 1.7. הספק יבצע הדרכה פרונטלית על התוכנה עפ"י דרישת החברה.

2. פיתוח מאובטח

- 2.1. שימוש בתקן OWASP או מקביל שיאושר ע"י החברה.
- 2.2. שימוש בגרסאות מעודכנות ונתמכות של שפות הפיתוח.
- 2.3. העברת מסמך אפיון מערכת לאישור של החברה.
- 2.4. פיתוח המערכת בהתאם לדרישות האפיון.
- 2.5. ביצוע בדיקות מסירה ע"י הספק לוודא קיום דרישות אבטחת מידע באפיון.
- 2.6. מבדק חדירה למערכת לפני העברה לייצור.

3. הפרדת סביבות

- 3.1. סביבת הייצור תופרד מסביבות אחרות.
- 3.2. העברת אפליקציה מסביבת פיתוח לייצור תתבצע בצורה מבוקרת.
- 3.3. לא יעשה שימוש בנתונים אמיתיים בסביבת הפיתוח.

4. הגנה אפליקטיבית

- 4.1. יכולת להגדיר הרשאות על פי פרופיל ולמדר גישה/עדכון ברמת שדה.
- 4.2. יכולת הפקה יזומה של דו"ח הרשאות תקפות אחת לשנה.
- 4.3. קישור ל-AD של קנט או לחלופין יישום מדיניות סיסמאות:
- 4.4. מינימום תווים בסיסמה -7
- 4.5. שילוב אותיות וספרות
- 4.6. החלפה אחת ל-180 יום
- 4.7. היסטוריה -10 דורות
- 4.8. נעילת משתמש לאחר 5 ניסיונות גישה שגויים –שחרור אוטו' לאחר שעה או ע"י ADMIN
- 4.9. חסימת משתמש שלא הזדהה 180 יום
- 4.10. הצפנת הסיסמאות בבסיס הנתונים ברמה של 256 ביט ומעלה
- 4.11. מניעת השלמה אוטומטית של הסיסמה.
- 4.12. הגדרת רשימת ערכים וטווחים מותרים לשדות קלט (כולל הגנה על FORM באמצעות CAPTCHA)
- 4.13. אין לחשוף למשתמש הקצה הודעות שגיאה אפליקטיביות העלולות להסגיר קוד וטבלאות בתוך היישום. שגיאות כאלה יש לכתוב לקובץ לוג בלבד או לתת הודעה גנרית.
- 4.14. במקרה של העלאת קבצים למערכת: יש לוודא כי קובץ העולה לשרת יעבור סניטציה ויישמר בשרת כקובץ בעל סיומת לא פוגענית כגון html ו/או php.
- 4.15. לאחר פרק זמן של אי-קיום פעילות לנתק את הפעילות/ התקשרות. ושברירת המחדל לסיום Session תהיה 60 דקות.

5. בקרת פלט

- 5.1. לוודא שאין בדוחות המופקים מהמערכת חשיפה של שדות שלא נדרשים
- 5.2. סיסמאות לא יוצגו על המסך

6. הגנה ברמת תקשורת

- 6.1. מימוש TLS1.2 ומעלה בלבד בין החברה לשרתי המערכת במקרה של ממשקי נתונים
- 6.2. יוזמת התקשרות הספק מרחוק למערכת תהיה אך ורק של החברה, והגישה תינתן באישור החברה בלבד.
- 6.3. על ההתקשרות מרחוק של הספק יחולו הכללים הבאים:
 - 6.3.1. הגדרת שם משתמש אישי לכל משתמש מטעם הספק
 - 6.3.2. הצפנת תווך הגישה
 - 6.3.3. ניטור פעולות הספק במערכת
 - 6.3.4. גישה לשרתי המערכת באמצעות חוק FW ייעודי מול הספק.

6.4. תיעוד בלוג:

- 6.4.1. נעילות משתמש
- 6.4.2. פעולות עדכון ע"י המשתמשים כולל שמירת ערך קודם.
- 6.4.3. העלאות תכנים
- 6.4.4. שינויים בהרשאות.