

2.19 אבטחת מידע

מאגר המידע של האסירים ברשות ברשת ינוהל ויאובטח כנדרש בחוק הגנת הפרטיות, התשמ"א-1981.

2.19.0 כללי

רמת אבטחת המידע בחברה צריכה להיות גבוהה על מנת לא לאפשר העברת נתונים מאובטחת ללא ביצוע מניפולציה על הערכים.

כמו כן הכניסה למערכות רק באמצעות זיהוי אישי של העובד לשם מניעת כניסה של אנשים לא מורשים.

2.19.1 סיכוני אבטחת מידע (במ"ם)

א. אפשרות של חדירות שונות כגון התקפות וירוסים ותולעים שונים, חדירה לא מורשית בגישה מהאינטרנט.

ב. כניסה של גורמיים לא רצויים דרך מחשבי הארגון לתוך המערכת

א. טעות אנוש העלולה להזיק לנתוני המערכת.

ב. לוגים – המערכת תנהל רישום כניסות ויציאות של משתמשים למערכת. המערכת תרשום כל עדכון שנעשה (כולל ע"י משתמש), וכן את תאריך העדכון.

2.19.2 אמצעי אבטחת מידע (במ"ם)

- ההגנה תמומש, בין היתר, באמצעות תוכנות אנטי וירוס עדכניות.
- שימוש ב FIREWALL לחסימה של גורמים לא רצויים לתוך הרשת הפנימית.
- עבודה ברשת תחת נוהל הסיסמאות מסודר.
- משתמש לא יוכל לעדכן או לתשאל מסד נתונים, אלא בגישה אפליקטיבית (באמצעות Service).
- קיום ניהול הרשאות תקני בהתאם לנהלים.
- הפרדה בין סביבת ייצור לפיתוח.
- הגנה על קוד מקור וספריות מערכת.
- אבטחת מערכת ההפעלה בהתאם לנוהל הקשחת שרת.
- קיום ושמירת אמצעי גיבוי רלוונטיים.
- קיום בקרה על אמצעי אבטחה ושימוש בקבצי ה-LOG.
- מעבר תקופתי על קבצי LOG של המערכת.
- הטמעת אמצעים למניעה ואיתור אירועי אבטחה (לדוגמה תוכנות אנטי – וירוס, תוכנות לגילוי ניסיונות פריצה וכו').

2.19.3 ניהול האבטחה

1. אבטחה פיזית:
בודד את הזרים / אורחים בארגון.
השיטה: חובת ענידת תגים לכל. תג עובד שונה ויזואלית באופן בולט מתג אורח / מבקר. בנוסף, יש לוודא כי מידע מסווג איננו ניתן להשגה מקרית על ידי בלתי מורשה.
 2. אין להשאיר מרווח לשיקול דעת במתן תמיכה בנושא סיסמאות / הזדהות כלפי הגורם נותן תמיכה. אין להעביר סיסמא באופן שאיננו מבטיח כי היא מועברת רק למי שזכאי לקבלה כדין. לדוגמא: קבע מערכת הזדהות חליפית אקראית, חייב הזדהות פיזית במקרים מסוימים וכדו'.
 3. מול כל גורם נותן תמיכה (בנוסף ל – Help Desk), יש לבסס שיטות להזדהות, הן של המשתמש והן של גורם התמיכה.
 4. הצב מגרסות במספר מספיק ובפריסה ארגונית מתאימה.
 5. קבע מדיניות והנהג נהלים. על מנת שאילו יהיו אפקטיביים עליהם לכלול:
 - נהלים הניתנים למימוש בלבד.
 - לתמצת כללי התנהגות לעובדים: בעיקר "עשה" (ואל תרבה ב"אל תעשה").
 - להתעדכן תקופתית.
 - נגישות לכל העובדים דרך אינטרא-נט.
- והעיקר: מודעות ועוד מודעות לעובדים ולמנהלים בכל עת: בעת קבלה לעבודה, בעת פגישות הנהלה, בעת פגישות מחלקתיות / צוות.