מסגרת זו תוחלף בהבהקים העיקריים של ה...., לפי שיקול דעת כותב המסמך ובהתאם לכללים הנהוגים בארגון.

**שימוש בגלופה זו מותנה ברישוי מפת"ח**

תוכן העניינים

[1. כללי 2](#_Toc401070111)

[2. עקרונות אבטחת מידע כלליים 2](#_Toc401070112)

[3. מדיניות מפורטת 2](#_Toc401070113)

[4. יישום המדיניות 3](#_Toc401070114)

# 1. כללי

## 1.1 מטרות

## 1.2 תכולה

# 2. עקרונות אבטחת מידע כלליים

## 2.1 העברת מידע רגיש

## 2.2 מנגנוני זיהוי ואימות הזיהוי

## 2.3 הכנסת אמצעי זיכרון חיצוניים למחשבי הארגון

## 2.4 הוצאת מידע ממחשבי הארגון

## 2.5 רישום אירוע חריג

## 2.6 כיבוי מחשבים בסוף היום

## 2.7 אחסון של מצעי זיכרון

## 2.8 דיווח לאחראי על אבטחת המידע

# 3. מדיניות מפורטת

## 3.1 בניית ארכיטקטורת רשת מאובטחת בהתאם לאיומים הרלבנטיים

## 3.2 ביצוע הקשחה של השרתים בארגון

## 3.3 ביצוע הקשחה של רכיבי התקשורת (נתבים, מתגים וכד')

## 3.4 התקנת אנטי וירוס לשרתים ולתחנות קצה

## 3.5 התקנה שוטפת של עדכוני תוכנה

## 3.6 שימוש במוצר להצפנת תעבורת האימייל מול ספקים רגישים

## 3.7 מדיניות לגבי סוג האימות של המשתמשים (סיסמה, כרטיס חכם וכד')

## 3.8 נטרול של כונני הדיסקטים וכונני ה-CD במחשבים

## 3.9 אוסף הנחיות של מותר ואסור עבור השימוש במחשב נייד

## 3.10 שימוש במנגנוני אבטחה באפליקציות ומסדי נתונים

# 4. יישום המדיניות

## 4.1 בדיקות אבטחה

## 4.2 בדיקות ארגוניות

## 4.3 בדיקות טכניות

## 4.4 איתור חולשות אבטחה

### 4.4.1 ניתוח התוצאות מבדיקת האבטחה

### 4.4.2 ביצוע בדיקות חדירות לרשת הארגון

### 4.4.3 שינויים והוספת מערכות ורכיבים חדשים

### 4.4.4 גילוי שוטף של חולשות אבטחה בעולם

## 4.5 עדכון מדיניות האבטחה