



מועצה אזורית הגלבוע
לשכת ראש המועצה

מועצה אזורית הגלבוע

תמצית מדיניות אבטחת מידע ISO 27001 ו- ISO 27799

1. רקע:

- 1.1 פעילותה התקינה של מועצה אזורית הגלבוע מושפעת ותלויה ברמת הסודיות, השלמות, הזמינות, התקפות הכלילות (Integrity) או השרידות של המידע והנכסים שבאחריות החברה.
- 1.2 המידע, המערכות המנהלות אותו, האמצעים והציוד עליו הוא מושתת, מהווים נכס מרכזי וחיוני של החברה ויש להגן עליהם בדומה למשאבים אחרים בעלי ערך לחברה.
- 1.3 פגיעה במידע תוביל לנזקים העלולים לתת אותותיהם בהיבטים תפעוליים, טכנולוגיים וכספיים וכן להוביל לפגיעה בצנעת הפרט של אזרחי המדינה, לפגיעה במוניטין ובתדמית הארגון והמדינה.
- 1.4 מדיניות אבטחת המידע מבוססת על סיכוני האבטחה הדינמיים, תוך התאמה לצרכים התפעוליים והארגוניים של הארגון. העקרונות המונחים במדיניות אבטחת המידע מהווים בסיס לנהלי העבודה בתחומי אבטחת המידע השונים.
- 1.5 מדיניות אבטחת המידע של החברה נגזרת מתקן ניהול אבטחת המידע הבינלאומי ISO27799 ותקן ISO27001.

2. מנהיגות ומחויבות הנהלה לנושא אבטחת מידע:

- 2.1 הנהלת המועצה (להלן: "ההנהלה") רואה את ההגנה על המידע הרגיש בארגון בהיבט של שלימות, זמינות ואמינות, כנושא בעל חשיבות עליונה.
- 2.2 הנהלת המועצה לוקחת על עצמה להוביל ולהנחיל את כלל הנושאים והפעילויות הנדרשות על מנת לממש הגנה ראויה על המידע כפי שמתחייב עפ"י דרישות החוק ותקן ISO 27799 ו- ISO 27001.

עמוד 1 מתוך 5



מועצה אזורית הגלבו
לשכת ראש המועצה

מועצה אזורית הגלבו

תמצית מדיניות אבטחת מידע ISO 27001 ו- ISO 27799

2.3 הנהלת המועצה תפעל במסגרת המשאבים הקיימים, על מנת להגן על המידע ועל הנכסים של הארגון, ולעמוד בדרישות מערכת ניהול אבטחת המידע (מנא"מ) כפי שמתחייב

בתקן ISO 27799 ו- ISO 27001.

2.4 על עובדי המועצה להיות מודעים לסיכונים של חשיפת מידע, לעשות את כל האמצעים כדי למנוע חשיפה, וככל שיתקלו באירוע חריג עליהם לדווח על כך לגורמי אבטחת המידע במועצה.

3. להלן מטרות אבטחת המידע בארגון:

3.1 הבטחת סודיות המידע החסוי והחסוי ביותר של תושבי ולקוחות המועצה, המטופל ונאגר במערכות המידע ומתקני החברה.

3.2 הבטחת זמינות המידע ומערכות המידע, לצורך המשכיות הפעילות הציבורית ומתן השירות לתושבים ללקוחות.

3.3 הבטחת אמינות המידע לאורך כל תהליכי העבודה במועצה ווידוא מתן תוצאות אמינות ומדויקות לכל התושבים ולקוחות.

3.4 אבטחת המידע העסקי הרלוונטי לפעילות המועצה.

3.5 אבטחת המידע האישי וחסיון המידע האישי של תושבי המועצה.

3.6 עמידה ברגולציות ונושאי אבטחת מידע מחייבים.

3.7 העלאת מודעות לאבטחת מידע בקרב מנהלים ועובדים והעלאת הכשירות המקצועית של העוסקים בתחום אבטחת המידע במועצה.

3.8 שיפור החוסן של מערכות המידע ורשתות הארגון בפני פגיעה בהיבט סודיות, אמינות וזמינות כתוצאה מפעילות זדונית ע"י גורם חיצוני או פנימי.

עמוד 2 מתוך 5



מועצה אזורית הגלבוש
לשכת ראש המועצה

מועצה אזורית הגלבוש

תמצית מדיניות אבטחת מידע ISO 27001 ו-ISO 27799

4. עיקרי שיטת הערכת הסיכונים

4.1 עקרונות מדיניות אבטחת המידע יתבססו על מערכת ניהול סיכונים, המזהה, מבקרת ממזערת או מונעת, את סיכוני האבטחה העלולים להשפיע על המידע, מאגריו או מערכותיו.

5. אחריות על אבטחת מידע במועצה

- 5.1 הנהלת החברה הגדירה את הגורמים והמסגרות הארגוניות, אשר באחריותם ליישם את מדיניות אבטחת המידע במועצה:
- 5.2 ועדת היגוי לנושא אבטחת מידע – מגדירה את מדיניות ונהלי המועצה בתחומים הנוגעים לאבטחת מידע.
- 5.3 ממונה אבטחת מידע - ממונה אבטחת מידע במועצה אחראי על הניהול השוטף של ענייני אבטחת מידע במועצה.
- 5.4 מנהלי ועובדי המועצה - על כלל מנהלי ועובדי המועצה חלה אחריות אישית בכל הנוגע לשמירה על אבטחת המידע וחסיונו.

6. על מנת לממש את אחריותה ומחויבותה של ההנהלה לנושא

אבטחת המידע הוגדרו ונקבעו הכללים לטיפול בנושאים

הבאים:

- 6.1 אבטחה לוגית - האבטחה הלוגית מהווה את ה"שכבה" העיקרית והקרובה ביותר בהגנה על המידע המצוי במערכות המחשב והתקשורת. ממונה אבטחת מידע בחברה יתווה

עמוד 3 מתוך 5



מועצה אזורית הגלבו
לשכת ראש המועצה

מועצה אזורית הגלבו

תמצית מדיניות אבטחת מידע ISO 27001 ו-ISO 27799

את רמת האבטחה הלוגית המחייבת עבור רכיביהן השונים של מערכות המחשוב והתקשורת. תיושם מדיניות הרשאות ובקרת גישה למידע בהתאם לתפקיד והצורך המקצועי.

- 6.2 אבטחה פיזית - ייושמו הגנות ובקורות פיזיות, על מנת למנוע פעולות אשר תוצאותיהן עשויות להיות חשיפה, גניבה, שינוי או הרס של מידע. אמצעי הגנה אלו יתאימו לרמת הסיווג של המידע.
- 6.3 אבטחת משאבי אנוש – נקבעו עקרונות אבטחת מידע בכל הקשור לעובדי המועצה, על מנת לצמצם את הסיכונים הנובעים מבעיות במהימנות עובדים, חוסר מודעות של עובדים או רצון מכוון של עובד לפגוע במידע האגור במערכות הארגון.
- 6.4 פיתוח מאובטח – הוגדרו היבטי אבטחת מידע ששולבו בתהליכי פיתוח מערכות מידע. אבטחת מטופלים ולקוחות ייושמו הגנות ובקורות הנדרשות על מנת למנוע פעולות שתוצאותיהן עלולות להיות חשיפה, גניבה שינוי או הרס מידע רגיש על תושבי הגלבו ולקוחות המועצה. אמצע הגנה אלה יתאימו לרמת הסיווג של המידע בארגון.
- 6.5 רכש וספקים – מיושמים היבטי אבטחת מידע בתקשורת ועבודה עם ספקים חיצוניים.
- 6.6 גיבויים – במועצה הוגדרו תהליכים להבטחת אמינות, שלמות, זמינות וכלילות (Integrity) המידע, וזאת ע"מ להבטיח שסוגי המידע השונים הקיימים במועצה מזהים, וכי דרישות גיבוי לכל סוג של מידע מוגדרות בהתאם לרגישות המידע.
- 6.7 בקרת גישה – נקבעו כללים ועקרונות למתן גישה ולמערכות המידע ובקרה אחר התחברות לרשת.

עמוד 4 מתוך 5



מועצה אזורית הגלבו
לשכת ראש המועצה

מועצה אזורית הגלבו

תמצית מדיניות אבטחת מידע ISO 27001 ו- ISO 27799

6.8 עבודה מרחוק – בחברה נקבעו כללים והנחיות אבטחת מידע לגישת עובדי המועצה וגורמים חיצוניים לרשת המועצה מרחוק.

6.9 אבטחת אמצעי מחשוב ניידים – מבוצע יישום העקרונות, השיטה, תהליכי העבודה והאמצעים ע"מ לאפשר שימוש מאובטח במחשבים נישאים/ניידים ולמנוע פגיעה בשלמות, אמינות, זמינות, סודיות ושמידות המידע המאוחסן על גבי מחשבים ניידים במועצה.

עמוד 5 מתוך 5

www.hagilboa.org.il □ e-mail: oved@hagilboa.org.il

מועצה אזורית הגלבו, ד.ב. גלבו 1894400 מוקד אזורי 109, טל. 04-6533200, פקס. 04-6531451