Fahn Kanne
Grant Thornton
An instinct for growth™

לשכת יועצי מס בישראל
INSTITUTE OF TAX CONSULTANTS IN ISRAEL

פאהן קנה Academy

רו"ח עדי שפיר, CRISC, CISA
מנהלת מחלקת ביקורת ויעוץ IT, פאהן קנה ושות'
Grant Thornton Israel

סוגיות בניהול טכנולוגיות מידע בחברה

הקדמה

ההתקדמות הטכנולוגית, קצב העסקים התכוף והצורך בנגישות גבוהה למידע,

"בעידן הכפר הגלובלי", הכתיבו מדיניות אשר הולכת ומשתנה ללא הרף, בתחום טכנולוגיות המידע.

- העלאת הצורך הגובר בשימוש בכלים מתוחכמים וניהול מערך טכנולוגיות ארגוני, הינו מהותי ליכולתו של התאגיד ליזום, להתפתח, להתחרות ולהתנהל ברמת היום יום ובסביבה העסקית הדינמית.
- כיום מכלול המידע הקריטי בארגון שמור במערכות המידע.
- הגנה על נכסי המידע הארגוניים והתשתיות, מהווה כיום את אחד הנדבכים החשובים בבניין תשתית טכנולוגית ואבטחת המידע.

©2019 Fahn Kanne & Co. Grant Thornton Israel. All rights reserved.

אבטחת מידע System Security

הגדרה: ענף העוסק בהגנה מפני גישה, שימוש, חשיפה, ציתות, שיבוש, העתקה או השמדה של מידע ומערכות מידע מצד גורמים שאינם מורשים או זדוניים.

"מטרות על":

- שלמות המידע
- אמינות המידע
- סודיות המידע
- זמינות המידע

מטרות אלו מחויבות ליישום והטמעה בכל ארגון, ללא תלות בגודלו, בסוג המידע או בצורת אחסונו

©2019 Fahn Kanne & Co. Grant Thornton Israel. All rights reserved.

איתור מוקדי הסיכון

- מיפוי נכסי המידע בארגון ואיתור הנכסים הקריטיים
- מיפוי תהליכים עסקיים ואיתור התהליכים הקריטיים
- ביצוע סקר סיכונים בתחום טכנולוגיות המידע לאיתור מוקדי הסיכון. הסקר בוחן את הסיכונים האפשריים בכל תחום טכנולוגיות המידע.

©2019 Fahn Kanne & Co. Grant Thornton Israel. All rights reserved.

הגנה על נכסי המידע הארגוני
Information Assets Protection

הגנה על נכסי המידע כוללת מספר מישורים:

- **אבטחה פיזית** - הינה אבטחת המבנה שבו נמצאות מערכות המחשוב, מערכות החומרה והתוכנה, רכיבי התקשורת, ובסיסי הנתונים (חדר שרתים).
- **אבטחה לוגית** - הינה אבטחה של מערך המידע, באמצעות שימוש בכלי אבטחת מידע שונים כגון: אנטי וירוס, חומת אש, הצפנת מידע, סריקה וניקוי של איומים, חסימת אתרים חשודים ועוד.

רמת אבטחת המידע הנדרשת בכל ארגון נקבעת על בסיס הנכסים הקריטיים אשר הוגדרו.

©2019 Fahn Kanne & Co. Grant Thornton Israel. All rights reserved.

הגנה על נכסי המידע הארגוני
Information Assets Protection

מנגנוני הגנה על נכסי מידע:

- ביצוע סקרי סיכונים תקופתיים בתחום אבטחת מידע.
- ניהול הרשאות ומשתמשים והפרדת תפקידים (SOD).
- מדיניות ניהול גיבויים ושחזורים.
- גיבוש תכנית המשכיות עסקית (BCP).
- גיבוש תכנית התאוששות מאסון (DRP).

©2019 Fahn Kanne & Co. Grant Thornton Israel. All rights reserved.

סקר סיכוני אבטחת מידע
Information Security Risk Survey

הגדרה: סקר הסיכונים מציג את התרחישים האפשריים לסיכונים שהוגדרו, מחשב את רמת הסיכון ונותן המלצות לצמצום הסיכון הגלום.

מטרה: בחינת הסיכונים האפשריים בתחום אבטחת המידע ומיפוי הסיכונים המהותיים.

בין הסיכונים העיקריים שנבחנים הינם:

- הפסד כספי.
- פגיעה בשירות לציבור.
- אי עמידה בהוראות חוק רגולציה.
- פגיעה במוניטין.

©2019 Fahn Kanne & Co. Grant Thornton Israel. All rights reserved.

ניהול הרשאות ומשתמשים
Permissions and Users Management

הגדרה: ניהול של חשבונות המשתמשים והרשאותיהם במערכות המידע השונות ובסיסי הנתונים, תוך שמירה על אחידות ואכיפת נהלי אבטחת מידע הנהוגים בחברה.

מטרה: להגן על נכסי המידע בחברה תוך מניעת מעילות והונאות.

ניהול מערך הרשאות במערכות המידע בארגון בהתאם לעקרון "הצורך לדעת" - הגבלת הגישה למידע לבעלי התפקידים הזקוקים להרשאות אלו בלבד ויישום עיקרון הפרדת תפקידים (Segregation Of Duties)

דוגמאות

- כאשר עובד עוזב את החברה יש לנטרל את חשבונות המשתמש שלו ולשלול את הרשאותיו בהתאם.
- יש להעניק הרשאות לעובדים על פי תהליך מסודר (טופס טיולים) לאפיון דרישה להרשאות ולבצע בקרה עוקבת על מנת לוודא כי העובד אכן קיבל את ההרשאות המתאימות.

©2019 Fahn Kanne & Co. Grant Thornton Israel. All rights reserved.

ניהול הרשאות ומשתמשים- "עקרון הפרדת התפקידים"

עיקרון הפרדת תפקידים (**Segregation Of Duties/Separation Of Duties**) קובע הפרדה בין הגורמים השונים האחראים לביצוען של פעולות בארגון כגון הפרדה בין גורם מבצע, מאשר ומבקר.

המטרות העיקריות ביישום של מערך הרשאות נאות ועיקרון הפרדת התפקידים בארגון הינן הגבלת סמכויות וצמצום תלות אפשרית בגורם בודד.

שמירה על עקרונות מנחים אלו יאפשרו צמצום הסיכון למקרי הונאות ומעילות.

להלן מספר דוגמאות:

- לעובד בעל מספר הרשאות: יצירת חשבון ספק, הזנת חשבונית והעברת אישורה לתשלום - יאפשרו ליצור ספק פיקטיבי במערכת, להזין עבורו חשבוניות ולבצע תשלומים במרמה.
- עובד בעל הרשאה לשינוי פרטי חשבון הבנק של ספקים והרשאת ביצוע תשלום לספק - יכול לבצע שינוי בפרטי חשבונות בנק לחשבונו הפרטי לפני ביצוע התשלום.

©2019 Fahn Kanne & Co. Grant Thornton Israel. All rights reserved.

ניהול גיבויים ושחזורים Backup And Restore Management

הגדרה: נוהל ליצירת עותק של נתונים בארגון והיכולת לשחזרו בעת הצורך.

היערכות נכונה, וניהול מדיניות גיבויים רציפה, תאפשר לארגון לשחזר את המידע תוך פרק זמן נתון ובכך להשיב את יכולתו להמשיך ולנהל את פעילותו העסקית השוטפת.

מטרה: הגיבוי נועד לשמירה על הנתונים של הארגון ושחזורם בשעת הצורך.

דרכים ליישום:

- שמירה על גבי שרת מקומי.
- ביצוע "רפליקציה" של נתונים לאתר מרוחק (DR)
- גיבוי בשרתי ענן
- ביצוע שחזורים יזומים לבדיקת תקינות התהליך
- ועוד...

©2019 Fahn Kanne & Co. Grant Thornton Israel. All rights reserved.

תכניות המשכיות עסקית והתאוששות מאסון (BCP / DRP)

הגדרה: תכניות להמשכיות עסקית (Business Continuity Plan) ולהתאוששות מאסון (Disaster Recovery Plan) פותחו בעבור ארגונים ככלי בכדי לאפשר את שמירת יכולותיו של הארגון לספק מוצרים ושירותים ללקוחותיו בקרות משבר, על רמת פעילותו השוטפת, וניהולו הרציף באמצעות הפעלה מחדש של שרותי טכנולוגיות המידע לרבות רכיבי התשתית, תקשורת והמערכות הארגוניות השונות.

התכנית מגדירה את האופן שבו הארגון יתנהל במצבי חירום ומדמה תרחישים שונים, וזאת בכדי להגן על נכסיו הקריטיים ולהבטיח את המשך קיומו.

©2019 Fahn Kanne & Co. Grant Thornton Israel. All rights reserved.

תכנית להתאוששות מאסון - DRP

הגדרה: תכנית התאוששות מאסון **Disaster Recovery Plan** הינה תכנית הכוללת תהליכים, מדיניות ונהלים המשמשים להתאוששות מאסון, תוך פירוט המשאבים והפעילויות הנדרשות.

תכנית זו מתמקדת בתחום טכנולוגיות המידע ומהווה חלק מתכנית המשכיות עסקית.

מטרה: הפעלה מחדש של שירותי טכנולוגיית המידע לרבות רכיבים כגון תשתיות, תקשורת, מערכות, יישומים ונתונים.

מערכות המחשוב המודרניות הפכו למרכיב הכרחי לביצוע פעילות עסקית בעבור תהליכים עסקיים.

הפסקה עבודת מערכות המחשוב כתוצאה מאסון, עלולה לגרום נזק כספי משמעותי לארגון ופגיעה במוניטין.

©2019 Fahn Kanne & Co. Grant Thornton Israel. All rights reserved.

תכנית להמשכיות עסקית - BCP

הגדרה: תכנית המשכיות עסקית **Business Continuity Plan** הינה תכנית שפותחה בעבור הארגון בכדי לאפשר לארגון להמשיך ולספק את מוצריו החיוניים ושירותיו ברמה המוגדרת מראש בקרות משבר.

בתכנית יוגדרו הדרישות העסקיות להמשכיות הפעילות.

מטרה: הפעלה מחדש של התהליכים הקריטיים בארגון עד לחזרה מלאה לשגרה, לשם שמירה על רציפות תפקודית.

התכנית מגדירה את האופן שבו הארגון מתנהל במצבי חירום, מדמה תרחישי חירום שונים בכדי להגן על רציפות תפקודית של תהליכי העבודה הקריטיים בארגון.

התכנית משתנה ומתאימה את עצמה לארגון בכדי לספק הגנה לארגון ולהבטיח את המשך קיומו גם לאחר מצב חירום.

©2019 Fahn Kanne & Co. Grant Thornton Israel. All rights reserved.

Fahn Kanne
Grant Thornton
An instinct for growth™

מחלקת ביקורת וייעוץ מערכות מידע

עסקית והתאוששות
- ניהול מערך הרשאות תקין מבוסס SOD
- סקרי סיכוני אבטחת מידע
- ניהול, בחינה והטמעת מדיניות אבטחת מידע בארגון

אבטחת מידע
- בחינת ניהול מערך גיבויים בהתאם לדרישות וצרכי הארגון
- בניית תכנית BCP
- בניית תכנית DRP

ניהול סיכוני מערכות מידע - IT
- הטמעת ERM-מתודולוגיה לניהול סיכונים
- סקרי סיכונים בתחום מערכות המידע
- איתור סיכוני מעילות והונאות
- יישום מערכות GRC לניהול סיכונים והרשאות

IT Advisory
- בדיקת דיוק ושלמות ממשקים בין מערכות ותהליכים בארגון
- ניתוחי נתונים
- הטמעת מתודולוגיות
- עמידה בחוק ורגולציה

©2019 Fahn Kanne & Co. Grant Thornton Israel. All rights reserved.

תודה על ההקשבה

רו"ח עדי שפיר **CRISC ,CISA**
מנהלת מחלקת ביקורת וייעוץ מערכות מידע
פאהן קנה ושות' Grant Thornton Israel
טל': 03-7106630
מייל: Adi.Shafir@il.gt.com

©2019 Fahn Kanne & Co. Grant Thornton Israel. All rights reserved.