

1	EPR מערכות בע"מ	
2	אבטחה פיסית	.1
2	אבטחה לוגית	.2
2	הפרדת מאגרי מידע	.3
3	מדיניות הוצאה משירות של מדיה מגנטית	.4
3	סדרי ניהול של מאגר מידע	.5
3	ניהול הרשאות	.6
3	6.1 אופן מתן הרשאת גישה למאגר המידע	
4	6.2 רישום מעודכן של מורשי הגישה	
4	תפעול	.7
4	סודיות	.8
4	בקרה	.9
5	מערכות בקרה:	
5	קבלת עובדים	.4
6	נספח – מדיניות סיסמאות	
6	מדיניות סיסמאות	1.
6	נעילת משתמשים	.2
7	מסמכים מקושרים והצפנה	.3
7	ניהול שגיאות	.4
7	חיווי ובקרה	4.10
9	נספח – שרידות	
9	מדיניות גיבויים	.1
9	רציפות תפקוד (DRP)	.2

1. **אבטחה פיסית** - קיום הגנה פיסית על מערכת המידע ועל התשתית שלה לרבות מבנה, אמצעי תקשורת, מסופים ותשתית חשמלית, מפני סיכונים סביבתיים ופגיעות התואמים את רגישות המידע שיעובד

המידע נמצא בחוות השרתים ב-AWS פרנקפורט ומופרדת, שרתים וירטואלים שונים יוזרים שונים לכל רשות והרשאות גישה בהתאם ליוזרים ולשרתים, כמובן שיש גבויים לאזורים שונים (ZONE) בתוך פרנקפקוט ועבודה במערכת ELB לטובת ניטור וחלוקת עומסים בין השרתים ולטובת שרידות מידית בנוסף לנל ישנה מערכת אוטמטית לגבויים לחוות שרתים נוספת באירלנד לטובת גיבוי במקרה של פגיעה ב-AWS פרנקפורט .

עוד הסבר ופרטים נוספים על האבטחה הפיזית והסביבתית על השרתים והתשתיות והתקשורת באתר AWS : <https://aws.amazon.com/compliance/data-center/data-centers>

2. **אבטחה לוגית** - נקיטת אמצעי אבטחה הולמים, בהתאם לרמת רגישות המידע, שימנעו חדירה מכוונת או מקרית למערכת או אל קווי התקשורת בין המזמין לקבלן

חברת EPR עובדת היום עם פרוטוקול מוצפן (HTTPS) המבטיח כי התעבורה שבין שהלקוח לשרת הינה מוצפנת, מה גם שעיקר העבודה מתבצעת בתחנות הקצה (שרתי טרמינל) אצלנו בחווה. במקביל, על מנת להתחבר לשרתי התוכנה (שבהם עובדים המשתמשים) יש להכניס 2 סיסמאות כניסה שונות. האחת לטובת חיבור לשרת והשנייה לטובת הפעלת התוכנה. כל הסיסמאות הינם סיסמאות קשות ומוצפנות ובעלות 8 תווים אותיות קטנות גדולות וסימנים, בהתאם למדיניות הסיסמאות (מצ"ב במסמך נפרד). חשוב לציין כי לשרתי EPR אין גישה מכל העולם, אלא רק בתנאי ש:

- IP מהארץ.
- רק לכתובת IP המוגדרות מראש .
- רק למחשבים שבהם הותקנה האפליקציה של EPR (שגם כדי להתקינה צריך 2 משתני הזדהות וסיסמא), והתערבות של מרכז התמיכה.

3. **הפרדת מאגרי מידע** - כללי הפרדת מערכות בין המערכות המקבלות גישה למידע, לבין מערכות אחרות בשימוש של הקבלן במהלך עסקיו

כיום המידע המופרד מתחלק למספר סוגים:

- הפרדה בין קבצים- ההפרדה מתבצעת ע"י Security Permeation ו Sher permeation.
 - הפרדה בין SQL DATA- בסיסי הנתונים השונים מופרדים ב Instances ברמת כל רשות, וההרשאות בחיבור וגישה לשרת הSQL הינם אך ורק ע"י Windows Authentications.
 - כמובן שכל רשות הינה קבוצה בעלת הרשאות גישה רק לנתונים ששייכים אליה הן ברמת בסיס הנתונים והן ברמת הקבצים .
- מיותר לציין כי כיום קיימת הקשחת שרתים, וכל שרת משמש אך ורק ליעוד הרלוונטי לו.

4. מדיניות הוצאה משירות של מדיה מגנטית ואופטית לרבות כוננים קשיחים, אמצעי אחסון ניידים או נתיקים, מצעי גיבוי וכדומה

היות ואנו עובדים בחוות השרתים של AWS – פרנקפורט נושא חיבור פיזי של מדיה מגנטית אינו שייך בגישה לשרתים, אלא רק ע"י חיבור מרוחק (ראו סעיף 1 אבטחה פיזית). כיום יש מערכת ניטור מידע בן שרתי הארגון לבין שרתי התמיכה ב-EPR כך שבמידה והמשתמש מנסה להוריד מידע המערכת מנתרת את הפעולה, וללא אישור של פורם אבטחת המידע לא ניתן להוריד מידע. במקביל כל המסמכים המצויים כיום בשרת הינם מוצפנים ולא ניתן לפתוח אותם ללא מפתח הצפנה ייעודי וייחודי.

בנוסף, מצד מדיניות האבטחה ב-EPR בכל הקשור להורדת נתונים למדיה מגנטית מחיבור מרוחק, הנהלים קובעים כי הנ"ל שלא בהוראת מנהל מאגר המידע הינו אסור. חשוב לציין כי גם על הרשות חלה החובה להדריך ולהסביר למשתמשי הקצה החשופים למידע רגיש – כיצד יש לנהוג בו.

5. נהלים - קביעת סדרי ניהול של מאגר מידע, סיווג והרשאות גישה למידע, והוראות לאיסוף, לסימון, לאימות, לעיבוד ולהפצה של המידע, בהתאם להוראות החוק והתקנות שמכוחו

כיום התוכנה עובדת התאם לדרישות החוק, ע"פ כל הסעיפים שפרטנו מעלה ומעבר להם. נהלי אבטחת המידע ב-EPR עובדו אישור עורך דין (עורך דין דן חי) - אשר מאשר מעבר לכל ספר כי חברת EPR הינה בית תוכנה העומד בדרישות החוק להגנת הפרטיות. יש לציין חברת EPR הינה חברה בין לאומית והיא מספקת שירותי תוכנה גם לרשויות בארצות הברית. רמות האבטחה שחברתינו נדרשת להם בחו"ל הינם והגבוהות שקימות היום היות ויש צורך בהצהרה לארגוני בריאות (בתי חולים וכ') - הצהרת HIPAA. במקביל חברת EPR עומדת בתקני ISO העולמיים (מטעם מת"י):

- 9001 - אמנת השירות
- 27001 – ניהול אבטחת מידע
- 27799 - אבטחת מידע לרשומות רפואיות

6. ניהול הרשאות:

6.1 קביעת אופן מתן הרשאת גישה למאגר המידע והטלת הגבלות על מורשי הגישה

המורשים להגיע למאגר המידע הינם אך ורק עובדים שמקימים תאים אלו:

1. עובד פעיל חברת EPR
2. חתום על הצהרת סודיות
3. הוא שייך למחלקת התמיכה של מערכות הרווחה ב-EPR או לחילופין איש סיסטם
4. בעל מאגר המידע או מנהל מאגר המידע או עובד מטעמו נתן את רשותו

6.2 עריכת רישום מעודכן של מורשי הגישה למאגר המידע לפי הרשאות הכניסה

השונות.

לחברת EPR סקר הרשאות עדכני. הסקר בחברתנו מתעדכן לפי שנויים בכ"א (גיוס או גריעה של עובד) או לחילופין שינויי כוח אדם בן מחלקתיים (עובד שעובר מתמיכה במערכת מידע אחרת של חברת EPR למערכות הרווחה וההיפך).
כמו כן כל התחברות לתוכנה או לבסיס הנתונים יוצרת לוג ותיעוד של:

- שם המחשב שממנו התבצעה הפעולה
- שם המשתמש בתוכנה
- שעת ההתחברות
- שעת ההתנתקות
- במידה ומדובר בניסיונות התחברות כושלים - המערכת מתעדת את מספר הניסיונות – לאחר 5 ניסיונות כושלים המשתמש ננעל – ולא ניתן יהיה לשחררו אלא באישור של מנהל המערכת המוגדר ברשות. הנעילה היא גם ליוזר וגם למחשב עצמו, לא ניתן להתחבר מאותו מחשב גם דרך יוזר אחר.

7. תפעול - קיום הוראות תפעול של המערכת תוך אבטחת המידע ושמירה על שלמות המידע

המערכת מתופעלת בצורה אוטומטית כך שבמידה ויש שגיאה, השגיאה מנוטרת - ומגיעה ישירות למחלקת הפיתוח לטובת תיקון וטיפול (מגיע במייל) כל הני"ל קורה לפי הנחיות אבטחת המידע ולטובת שמירה על שלמות הנתונים.

8. סודיות - החתמת מורשי הגישה על התחייבות לשמירה על סודיות ועל ההוראות שנקבעו לפי הנהלים ומסמך האבטחה

כל מורשי הגישה חותמים על הצהרת סודיות לשמירה על ההוראות שנקבעו ועל סמך הנהלים של חברת EPR. עובדי מרכז התמיכה של מערכת הרווחה הם המורשים הבלעדיים לגשת לבסיס הנתונים של מערכות הרווחה. ישנה גישה נוספת לאיש הסיסטם שלנו לטובת תחזוקה וDBA. אין שום גישה לבסיס הנתונים לכאלו שאינם מורשים.

9. בקרה - קביעת סדרי בקרה לגילוי פגיעות בשלימות המידע ותיקון ליקויים

המערכת ברמת כל תוכנה מריצה פעולות לתחזוקת המערכת.
המערכת מריצה תחזוקה קבועה לטיוב עבודה עם בסיס הנתונים, איש DBA בדק את בסיס הנתונים בצורה אקראית.
במקביל במידה ויש שבעיה בשלמות הנתונים המערכת מתריעה ושולחת מייל אל מחלקת הפיתוח עם השגיאה או השדה שחסר ופרטים על זמן ביצוע הפעול המשתמש והבעיה.

מערכות בקרה:

• Amazon CloudWatch

כלי ושירותי ניטור מעקב וניהול מבית אמצון המאפשר ניטור וניתוח על מנת להפיק תובנות בכדי לעקוב אחרי ביצועי המערכת ולייעל את ביצועי המערכת, ולהתריע בפני חריגים או עיוותים בהקצאת משאבים. המערכת מאפשרת להגדיר התראות נתונים וערכים שונים ברזולוציה גבוהה ובכך מאפשרת לפתור בעיות ולגלות תובנות ולייעל את השרתים שלנו.

• ELB-EPR

מערכת שרתים אלסטית לניטור וחלוקת עומסים בשרתי EPR. המערכת מנטרת את העומס על השרתים הזמינים ומחברת את המשתמש לטרמינל הפנוי ביותר.

• כלי ניטור ופיקוח עצמיים-

EPR מפעילה מערכות ניטור פנימיות וחיזוניות של Microsoft בעלות יכולת ניטור התראה לטובת פיקוח על עומסים בשרתים, עומס בזיכרון או בעיות שונות בשרת.

10. **קבלת עובדים** – קביעת תנאים לגבי אמינות עובדים ועבר של עבירות הקשורות בשימוש במידע בהתאם לרגישות המידע

חברת EPR הינה חברה שנמצאת בישוב קהילתי, עם מאפיינים של משפחתיות, העובדים בה מגויסים רק על סמך חוות דעת של עובדים שקיימים היום (עיקר העובדים גרים בישוב עלי ובסיבותיו), ובנוסף היכרות ובירור עם אנשים שמכירים את אותם עובדים (שכנים מקרים וכו'). כל נושא קבלת העובדים עומד בקריטריון של:

1. חבר מביא חבר.
2. בעל תואר אקדמי רלוונטי.
3. חתימה על חוזה אישי.
4. חתימה על מסמך הצהרת סודיות.
5. המלצות של עובדי חברת EPR או של המעסיק הקודם.
6. ראיון עבודה טלפוני.
7. ראיון עבודה ע"י מנהל מחלקה ומנהלת HR.
8. ראיון עבודה ע"י מנכ"ל החברה.

1. מדיניות סיסמאות

- 1.1 הסיסמא לא תעבור גלויה ברשת אלה בצורה מוצפנת \ ב hash או על גבי תווך מוצפן.
- 1.2 המערכת תספק למשתמש את היכולת להחליף את הסיסמא בעצמו, בצורה בטוחה, בכל עת.
- 1.3 סיסמת המשתמש לא תהייה קצרה מ 8 תווים ותהייה מורכבת מ:
 - אותיות קטנות.
 - אותיות גדולות.
 - ספרות.
 - תווים מיוחדים.
- 1.4 תוקפה של סיסמת המשתמש יפוג כל 180 יום ועל המשתמש יהיה להחליף את סיסמתו בהתאם למבנה המתואר לעיל.
- 1.5 מנגנון החלפת הסיסמא ישמור היסטוריית הסיסמאות של 2 מחזורים . ולא יתאפשר למשתמש לחזור על אף אחת מהסיסמאות הללו בעת החלפת הסיסמא.
- 1.6 טרם החלפת הסיסמא על המשתמש יהיה להקיש את שם המשתמש שלו ואת סיסמתו הנוכחית.
- 1.7 המערכת תחייב את המשתמש להחליף את סיסמתו הראשונית בעת ההתחברות הראשונה למערכת.
- 1.8 במקרה בו המשתמש שכח את סיסמתו, המשתמש ילחץ על כפתור שכחתי סיסמא ויקבל SMS לטלפון הנייד שלו סיסמא ראשונית לטובת הכנסת סיסמא חדשה.
- 1.9 יצירת סיסמא חדשה במקרה בו המשתמש שכח את הנוכחית תהייה אך ורק לאחר זיהוי המשתמש באמצעים אחרים, כגון שליחת SMS.
- 1.10 בשום שלב במחשבי המערכת, במחשבים של משתמשי המערכת, בקוד המקור של דפים וטפסים המועברים למשתמש, את מזהי האימות של המשתמשים השונים במערכת.
- 1.11 לאחר חוסר שימוש במערכת של 30 דקות המערכת תנעל והמשתמש יהיה מחוייב בהקשת הסיסמא.
- 1.12 סיסמת המשתמש תשמר בצורת hash בבסיס המידע.
- 1.13 הצפנת הסיסמא באלגוריתם Hash בטוחים Sha-256 או Sha-512.

2. נעילת משתמשים

- נעילת המשתמשים תתבצע לאחר 5 ניסיונות הזדהות כושלים.
- 1.14 השחרור יבוצע על ידי מנהל המערכת לאחר קבלת הפניה מהמשתמש ווידוי זהותו.
 - 1.15 נעילת המשתמש תתבצע כך שהמשתמש יהיה חייב להכניס שוב פעם את הסיסמא שלו והניתוק יתבצע בצד הלקוח.
 - 1.16 במקרה של נעילת משתמש, המשתמש יקבל חיווי כי עליו לפנות למנהל המערכת לטובת שחרור הנעילה

1.17 במקרה של ניסיון כניסה שגוי עם משתמש מסוים באותו מחשב או לחילופין עם אותו משתמש ממספר מחשבים שונים, המערכת תנעל את המשתמש להתחברות. בנוסף – במידה והני"ל בוצע מאותו מחשב גם המחשב ינעל להתחברות מ-EPR, לטובת שחרור הנעילה יהיה צורך בפניה למנהל המערכת.

3. מסמכים מקושרים והצפנה

המערכת מצפינה ב-HASH את כל המסמכים במערכת ע"י מפתח הצפנה ייחודי רשותי כך שלא ניתן לפתוח מסמכים המכילים מידע רגיש ישירות מהרשת.

4. ניהול שגיאות

1.18 הודעות שגיאה שיוצגו למשתמש כתוצאה משגיאות המתרחשות באפליקציה יהיו הודעות שאין בהן כדי לחשוף את אמצעי האבטחה במערכת. הודעות השגיאה אינם חושפות מידע רגיש בנוגע למבנה המערכת ומשאבי המערכת. הודעות השגיאה שיוצגו יהיו ג'נריות וכלליות.

1.19 הודעות שגיאה שיוצגו למשתמש יהיו הודעות שאין בהן כדי לחשוף את התשתית האפליקטיבית לגרסאותיה השונות כגון: מערכות הפעלה, שרתי web, שרתי אפליקציה, בסיסי נתונים, פרוטוקולים בשימוש, Web Services וכדומה.

1.20 המערכת לא מציגה מידע רגיש כולל: מספרי אשראי, סיסמאות, מפתחות הצפנה וכ"ו בהודעות שגיאה המוצגות למשתמש.

1.21 כאשר קלט המשתמש אינו מתאים לתבנית הנדרשת בשדה קלט, המערכת מציגה הודעת שגיאה המפרטת מהי התבנית בה נדרש להשתמש.

1.22 על המערכת לנהל מערך ללכידת שגיאות בזמן ריצה:

- יש לצפות שגיאות מראש וללכוד אותן בקוד המערכת.
- כל השגיאות מנוטרות בזמן אמת ומגיעות לכתובת המייל של האנשים הרלוונטיים בארגון

1.23 מידע משגיאות יהיה מתועד ע"י המערכת בטבלאות ה-log שלה.

1.24 ניתן להציג למשתמש קוד המתאים לרשומה בלוג לשם טיפול בשגיאה. קוד הרשומה לא ירמוז בשום צורה על קוד השגיאה והסיבה להתרחשותה לדג' "תקלה מספר 12215 אנא פנה לתמיכה"

1.25 המערכת מתמודדת עם שגיאות בהיבט של זמינות כך שאם למשתמש מסוים מתרחשת שגיאה הוא אינו חוסם גישה למשתמשים אחרים שמריצים את המערכת (קריסה כללית).

1.26 עבור כל שגיאה במערכת, המערכת מתעדת במידה ומוגדר:

- Timestamp
- זיהוי המשתמש (ללא סיסמא)
- מיקום המשתמש (שם מחשב)
- מיקום המשתמש במערכת (מסך, טופס, טבלה וכדומה)

1.27 חיווי ובקרה

המערכת מתעדת עבור כל פעולה:

- עדכון מידע במערכת.
- כתיבה ומחיקה של מידע במערכת.
- כל פעולות הניהול במערכת.
- כל פעולות הזיהוי במערכת, כולל כישלונות של פעולות אלו והסיבה לכך.
- כל פעולות ההרשאות במערכת, כולל כישלונות של פעולות אלו.
- שגיאות מערכת.

5. מדיניות גיבויים

חברת EPR מבצעת גיבויים שוטפים לטובת שיפור השרידות.

חברת EPR בחרה לעבוד עם AWS אמזון – פרנקפורט. קיים מערך גיבוי על בסיס שעתי, יומי, שבועי, חודשי עד 24 חודשים. על בסיס הנתונים יש גיבוי כל שעה שבעה ימים אחורנית וכל חודש למשך 24 חודשים.

במקביל את הגיבויים אנחנו מעבירים כל לילה לסביבת שרתים נוספת ונפרדת של אמזון באירלנד מידי יום. בנוסף בחוות השרתים שלנו באירלנד ישנם שרתים לטובת שיחזור והפעלה כך שבמידה וחלילה ישנה תקלה בשרתים בפרנקפורט הסביבה החלופית באירלנד מוכנה ליום פקודה.

אנשי ה-SYSTEM בחברת EPR דוגמים את בסיסי הנתונים בצורה אקראית מעת לעת לטובת בדיקת תקינות הגיבויים.

6. רציפות תפקוד (DRP)

מטרת התכנית להמשכיות עסקית BCP - Business Continuity Plan נועדה להבטיח רציפות תפעולית של התהליכים העסקיים הקריטיים של הארגון בשעת חירום בפרק זמן מוגדר וברמת שירות מוגדרת.

התכנית מתייחסת לאירועי חירום שונים ומגדירה תכניות פעולה לפונקציות הקריטיות בארגון לצורך התאוששות באופן מלא או חלקי בהתאם למדיניות הארגון.

כחלק הנושא השרידות EPR מחזיקה שרתי גיבוי ב-AWS אירלנד לטובת הקמה ושיחזור של סביבות עבודה במידה וחלילה יש תקלה בחוות השרתים ב-AWS פרנקפורט.

בנוסף חברת EPR עובדת עם שרתי טרמינל אלסטיים (ELB) המאפשרים שרידות מקומית מיטבית וכך במידה ושרת אחד קורס המערכת מעבירה את המשתמשים לעבוד על שרת אחר.