נספח י' - אבטחת מידע מערכת גניזה ואירכוב

1. כללי

1.1. פעילותה התקינה של חברת רכבת ישראל מושפעת ותלויה מרמת שלמותו, אמינותו, עדכניותו, זמינותו, שרידותו ושמירת סודיות המידע/מערכות.

1.2. המידע, המערכות המנהלות אותו, האמצעים והציוד עליו הוא מושתת, מהווים נכס מרכזי וחיוני של החברה ויש להגן עליהם כעל משאבים אחרים בעלי ערך בחברה.

1.3. פגיעה במידע, במאגריו לרבות חשיפה, חבלה או שיבוש, עלולים לפגוע בפעילות החברה עד לרמת השבתתה המלאה. הנזקים עלולים לתת אותותיהם בהיבטים מסחריים, עסקיים, שיווקיים, תפעוליים, טכנולוגיים וכספיים, עלולים להוביל לפגיעה במוניטין ובתדמית החברה.

2. הגדרות

2.1 **ר"י**-רכבת ישראל.

2.2 **ספק-**חברה אשר מספקת שירותי מחשוב בענן לרכבת ישראל.

2.3 **ארכיב** - אתר המשמש לאחסון רשומות אשר אינן נדרשות באופן שוטף אך נדרש לשמרן עפ"י חוק הארכיונים תשט"ו-1955 והתקנות הנגזרות ממנו.

2.4 **יחידת תיוק** – תיק, קלסר, מעטפה, צרור מסמכים, סרט וכיו"ב, המגדירים יחידת מידע בעלת מאפיין כגון שם או מספר.

2.5 **חומר ארכיוני** - כל כתב על גבי נייר או חומר אחר לרבות יחידת תיוק או מיכל אחסון.

2.6 **מיכל** - מיכל אחסון סטנדרטי מקרטון שמידותיו בס"מ 37 X 31 X 40 (כולל מכסה).

2.7 **הפקדה** – תהליך ההכנה של חומר ארכיוני והעברתו לשמירה בארכיון/מגנזה.

2.8 **תקופת שמירה** – פרק הזמן שבו מחויב ארגון לשמור את התיק/מיכל.

2.9 **אחזור/שליפה** – איתור יחידת תיוק הנדרשת על ידי המזמין והמצאתה למזמין בהתאם לנהלים שיקבעו עפ"י מכרז זה.

2.10 **נכס ר"י**, **חומרי ר"י**- מידע, מסמכים, שרטוטים, מדיה מגנטית וכו' השייכים לר"י.

2.11 **מידע-** כל נתון הנוגע ו/או הקשור לפעילותה, תפעולה או תפקודה של החברה, לרבות מידע הנוגע לצנעת הפרט של עובדי החברה, הקיים על-גבי אמצעי אחסון ממוחשבים, מגנטיים או אלקטרונים, ועל-גבי מצעי מידע פיזיים .

2.12 **איום** – Threat : אפשרות פוטנציאלית לפגיעה בשלמות, זמינות או חשאיות המידע.

2.13 אמצעי זיהוי-אמצעי המספק פרטים לגבי זהותו של אדם או מערכת בעת ניסיון כניסה ואישור ביצוע פעולות מטעמם למערכת מידע.

2.14 **הערכת סיכונים**-תהליך של הערכת רמת הסיכון של המערכות השונות בארגון. התהליך ממפה את האיומים השונים הנובעים מהפעילות במערכות השונות.

2.15 **זיהוי חד ערכי**- ערך ייחודי המזהה את מי שמתיימר להיות בעל אמצעי הזיהוי.

2.16 **חשיפה** – Vulnerability : חולשה במערכת העלולה להוביל להתממשות איום.

2.17 **לוג** – Log : קובץ התיעוד של נתיב בקרה.

2.18 **מידע רגיש**- מידע שר"י סיווגה כבעל סיווג הדורש אמצעי אבטחת מידע נאותים. בכל מקרה מידע בעל סיווג גבוה, יוגדר כמידע רגיש, תכולת מידע זה נתונה לפרשנותו של הארגון, אלא אם צוין אחרת במפורש בהוראה זו.

2.19 **מערכות מידע**- כלל הציוד הממוכן התומך בעיבוד מידע של ההחברה והספק הכולל בין השאר : שרתים, מחשבים נייחים ונייידים, ציוד תקשורת, ציוד אבטחת מידע.

2.20 **נתיב בקרה**- תיעוד פעולות המתבצעות במערכות מידע. קובץ התיעוד מקשר את הפעולה לנתונים נוספים כגון : שם מבצע הפעולה, המועד, הפעולה עצמה ועוד.

2.21 **סקר סיכונים**-סקר המאתר איומים/חשיפות הקשורות באבטחת מידע במערכות שונות והמעריך את רמת הסיכון שלהם לרכבת ישראל

3. <u>חוקי המדינה</u>

3.1. ספק המערכת ימלא במלואן כל ההוראות והחוקים במדינת ישראל כדוגמת:

3.1.1. חוק המחשבים

3.1.2. חוק הגנת פרטיות ותקנות העזר, ובכלל זה הנחיות רמו"ט.

3.1.3. חוקי דיני ראיות.

3.1.4. כל חיקוק עתידי לניהול מאגרי מידע ולשמירתם.

3.2. כל בירור והתדיינות בסוגיות משפטיות יתבצע יתקיים בבית המשפט בתל אביב, וזאת בהתאם לחוק הישראלי. למען הסר ספק, יאסר על הספק לעלות השגות בנושא סמכות משפטית ו\או סמכות דיונית מקומית.

3.3. הסעיפים הנ"ל יוכנסו בחוזה שיחתם רכבת ישראל לספק.

4. <u>חוזה</u>

4.1. הספק יתחייב שלא למסור\להעביר לגורם אחר כל מידע אשר יימצאו במערכותיו והינו שייך לרכבת ישראל.

4.2. הספק ידווח לרכבת ישראל במידה והיה אירוע אבטחת מידע ו\או אירוע הגנת פרטיות ממערכותיו באופן מיידי, אף אם למשנת הספק לא נגרם נזק ו\או חשיפה כתוצאה מהאירוע הנ"ל.

5. <u>סיום ההתקשרות</u>

5.1. הספק מתחייב, על פי דרישת הרכבת, להעביר את כל המידע והחומרים לרכבת ישראל או לספק אחר מטעמה.

5.2. הספק מתחייב, בתום ההתקשרות, להשמיד כל מידע השייך לרכבת ישראל המצוי ברשותו בתיאום עם רכבת ישראל.

6. <u>פרטיות</u>

6.1. הספק יתחייב לשמור\להגן על פרטיות מידע, נכסים (השייכים לר"י) אשר ישויכו לרכבת ישראל.

6.2. הספק יתחייב לעמוד בהתאם לחוק הגנת פרטיות ותקנות העזר.

6.3. כל שינוי במדיניות הספק בנוגע להגנת הפרטיות וכל הקשור לאבטחת מידע חומרי מידע הקשורים לר"י יובא לאישור ר"י.

7. <u>חוקיות התכנה ופלטפורמת מחשוב</u>

7.1. הספק יצהיר שכל התוכנות ומערכות המחשוב אשר משמשים אותו לבמתן השירותים לר"י הינם חוקיים, ונמצאים בבעלותו הבלעדית.

8. <u>זכויות חוזיות</u>

בהתאם לזכויות החוזיות, רשאית רכבת ישראל:

8.1. לדרוש דוח על ליקויים אבטחתיים ו\או ליקויים בתחום הגנת הפרטיות, במידה וקיים חשד ברכבת ישראל על קיומם.

8.2. להורות לחברה להפסיק העסקתו של עובד זה או אחר, מטעמים הנוגעים לביטחון מערכות המחשוב ומאגרי המידע הקשורים לרכבת ישראל.

8.3. לדרוש תיקון ליקויים , אשר יתגלו בסקרי סיכונים, ביקורות מתוכננות, ביקורות פתע , גילוי אקראי או יזום של ליקויי אבטחה, אשר יש להם השלכה על אבטחת מערכות רכבת ישראל– והחברה תהיה חייבת לתקן ליקויים אלו תוך פרק זמן סביר (לעניין זה - הזמן המוערך ע"י גופים מקצועיים לתיקון הליקוי). במקרי ליקויים קריטיים, תידרש החברה לתקן ליקויים אלו באורח מידי.

9. <u>אישור עבודה והצהרת סודיות</u>

9.1. נציג מורשה חתימה מטעם חברת האם, ונציג מורשה מטעם נציג חברת האם במדינת ישראל, יחתמו על הצהרת סודיות עבור הספק ובעצם חתימתם תייצג מחויבותו של הספק לעמוד בכלל ההתחייבויות החוזיות והחוקיות.

9.2. על הספק לפעול להסדרת אישור הפעילות של העובדים המטפלים בארכיון על מערכותיו, כפי הנדרש מכל עובד מיקור חוץ, ואשר כוללים גם בדיקה במרשם הפלילי של משטרת ישראל.

9.3. על הספק יהיה להחתים את עובדיו על הסכם סודיות וזאת לפני שהעובד ניגש למידע של ר"י .

9.4. כל טפסי הצהרת הסודיות יועברו לרכבת ישראל.

9.5. רק עובדים שאושרו מראש, ע"י אגף הביטחון – יוכלו לטפל בענייני הרכבת.

10. <u>קניין</u>

כל המידע, אשר יאוחסנו אצל בספק הינו בבעלותה המלאה והבלעדית של ר"י.

11. <u>אמנת שירות</u>

11.1. ר"י תקבע אמנת שירות עם הספק.

11.2. כל שינוי באמנת שירות יובא לאישור ר"י.

11.3. כל שינוי במדיניות אבטחת מידע אצל הספק בנוגע לחורים השייכים לר"י תובא לאישור בר"י.

12. <u>סיווג נכסים ,חומרים ר"י</u>

12.1. סיווג חומרים השייכים לרכבת ישראל מוגדרים בסיווג רגיש

13. נהלים

13.1. נהלים באחריות הספק

13.1.1. יצירת נוהלי אבטחת מידע העוסקים בין השאר ב:

13.1.1.1. אבטחת סביבה פיזית.

13.1.1.2. אבטחת נכסי מידע של הלקוח.

13.1.1.3. אבטחת יישומים של הלקוח.

13.1.1.4. שרידות, גיבוי, המשכיות עסקית.

13.1.1.5. אבטחה פיזית ולוגית

13.1.1.6. אבטחת רשתות.

13.1.1.7. אירועי אבטחת מידע, ניהול תגובה וכו'.

13.1.1.8. פיתוח ותחזוקה של המערכות

13.1.1.9. ביקורות.

13.1.1.10. הגנת פרטיות

13.1.1.11. נהלי טיפול משאבי אנוש (קבלה, עזיבה וכו')

13.1.2. הספק יעביר לרשות ר"י את כל הנהלים אשר ברשותו והקשורים לפעילות מול הרכבת.

14. מסירת מידע והסכם חסיון

14.1. הספק לא ימסור מידע ממאגרי המידע מחומרי ר"י, נשוא ההתקשרות זו לשום גוף או אדם, ללא אישור בכתב מאגף בטחון או מי מטעמו(ממונה אבטחת מידע).

14.2. אף אם הספק יקבל צו שיפוטי המתיר לגורם ממשל ו\או גורם צד שלישי לגשת למידע, חובה יהיה על הספק לאפשר לר"י להגיש התנגדות לצו, וזאת לפני מסירת המידע לגורם הממשל ו\או גורם צד שלישי.

14.3. הספק יערוך ויקיים נוהל רישום מסודר של העברה\קבלה מידע כלשהוא בנוגע לנכסי ר"י לגורם מוסר\מקבל מידע , תוך רישום פרטי המקבל\מוסר , סוגי רשומות ומועדי מסירה וקבלה , רישום הנ"ל יועבר מדי חצי שנה לעיון לאגף בטחון.

15. אבטחת מידע בניהול משאבי אנוש של הספק

15.1. אבטחת מידע בתהליכי גיוס עובדים

15.1.1. עובדים המגויסים לארגון יעברו בדיקות רקע, אשר מטרתן לאמת את הנתונים שנמסרו על-ידי המועמד/ת. במסגרת זו, תיבדק אמינות הנתונים.

15.1.2. עבור משרות רגישות הנוגעות במידע, כפי שיוגדרו על-ידי מנהל אבטחת המידע, יבוצעו בדיקות רקע ואמינות נוספות.

15.1.3. חוזה הנחתם עם עובדים חדשים יכלול התייחסות לאחריות העובד בכל הנוגע להיבטי אבטחת מידע, וילווה בהצהרת סודיות.

15.1.4. חוזה של הארגון עם חברות כוח אדם/השמה או עם חברות המספקות שירותי מיקור חוץ (Outsourcing), יכלול התייחסות בכל הנוגע לבדיקות המבוצעות בתהליכי גיוס העובדים.

15.2. אבטחת מידע בעת העסקת עובדים והגברת המודעות שלהם

15.2.1. נוהלי אבטחת מידע של הספק יגדירו מהן הפעולות שיש לבצע כדי לשמור על נכסי המידע של הארגון, פעולות אלו יכללו גם אמצעים שינקטו לגבי התקשרות של העובדים מחוץ למקום העבודה.

15.2.2. לגבי עובדים שיש להם נגישות למידע רגיש או מידע בעל סיכון גבוה, יוגדרו נהלים ברורים ויוגדר פיקוח לפעולות נוספות המיועדות למנוע את זליגת המידע.

15.2.3. הספק יגדיר תכנית הדרכה להעלאת רמת מודעות העובדים לאבטחת המידע בארגון.

15.2.4. לעובדים יינתנו הדרכות אבטחת מידע בהתאם למידת הידע הנחוץ לכל בעל תפקיד.

15.3. אבטחת מידע בסיום העסקת עובדים

15.3.1. לעובדים (כולל עובדים חיצוניים לארגון) המסיימים את העסקתם בארגון, בין אם ביוזמתם או ביוזמת המעסיק, ייחסמו הרשאות הגישה למידע (בין אם למערכות מידע ובין אם לאמצעים פיזיים).

15.3.2. ההספק יוודא כי בסיום ההעסקה לא יישארו נכסי מידע של הארגון בידי העובד.

15.3.3. הספק יגדיר את אופן הטיפול בעובדים בהיבטי אבטחת מידע לתקופת הזמן שבין הודעת העזיבה לסיום העסקה. יש להגדיר דרישות לפחות בנושאי בקרת גישה, עבודה על מערכות ומסמכים וכו'.

16. <u>אבטחה פיזית וסביבתית</u>

16.1. אזורים מאובטחים אצל הספק בשייכות לנכסי ר"י

16.1.1. הספק יחלק את סביבת העבודה למעגלי אבטחה/אזורים מאובטחים לפי רמות רגישות.

16.1.2. הספק יישם מספר מעגלים של בקרות גישה פיזית.

16.1.3. הספק יישם מערכת אבטחה משולבת באמצעים טכנולוגיים, הכוללות מצלמות, אמצעים ביומטריים, קוראי כרטיסים ואמצעי התראה מסורתיים, כגון מנעולים ומפתחות.

16.1.4. אמצעי בקרה תפעוליים ישולבו לצורך ניטור אוטומטי ומתן התראה במקרה ומתרחשת פריצה או בעיה.

16.1.5. ניהול גישה לנכסים פיזיים יבוצע באופן מרכזי אשר ישלב רשומות הניתנות לביקורת באמצעות ריכוז זרימת העבודה עבור תהליכים לבקשה, לאישור למתן גישה למרכזי נתונים.

16.1.6. ניהול גישה זה יפעל על פי עיקרון של מתן גישה מינימלית נדרשת וישלב תהליכי זרימת עבודה להשגת אישורים מגורמי אישור מרובים.

16.1.7. יבוצע תיעוד ודיווח בבקרת מרכז נתונים ראשי והעתק התיעוד והדיווח יומצא לר״י על בסיס שוטף.

16.1.8. הגבלת גישה לאנשי סגל של הספק-הגישה תוגבל באמצעות החלה של מדיניות של הרשאות סף כך שרק אנשים מורשים וחיוניים לנהל יישומים ושירותים של לקוחות בחלוקה לכל לקוח.

16.1.9. גישה של אנשי הספק לנתוני רכבת ישראל תידרש לשילוב של מספר גורמים לאימות.

16.1.10. כל ניסיון גישה חריג ושאינו בהתאם להרשאות אשר הוסכמו ואינו על פי אימות נדרש, יתוחקר וידווח לאגף בטחון רכבת ישראל (לממונה אבטחת מידע) במידי.

16.2. בטיחות

16.2.1. הארכיב יהיה מוגן מפני שריפה עפ״י דרישות העמידות באש .

16.2.2. בכל האולמות תותקן מערכת גילוי אש ועשן אוטומטים וידנית .

16.2.3. במבנה יותקנו מטפי כיבוי אש מטלטלים .

16.3. סביבה אקלימית נאותה

16.3.1. באולמות האחסון יקוימו תנאי האקלים נדרשים.

16.3.2. בכל אולם אחסון יותקן רשם לחות וטמפרטורה אחד לפחות ויתבצע פיקוח על הטמפרטורה, לחות היחסית ותנאי האוויר בתוך החלל.

16.3.3. תתבצע מניעת חדירת מים לאולמות האחסון.

17. <u>פיקוח ובקרה אצל הספק</u>

17.1. הפעילות בבית הארכיב תהיה כפופה להנחיות המקצועיות של נציג רכבת ישראל, ותתבצע תחת פיקוחו. המציע מתחייב לפעול בהתאם להנחיות אלה.

17.2. רכבת ישראל תהיה רשאית, על-פי שיקול דעתה, לערוך ביקורות על אופן מתן השירותים, על המצאי, על ניהולו ועל שיטת העבודה, באמצעים שתמצא לנכון.

17.3. המציע מתחייב לבקשת רכבת ישראל, להעביר לרכבת ישראל את כל המידע והנתונים הנמצאים בידיו בדבר פעילות הארכיב.

18. <u>אבטחת מידע לתשתיות טכנולוגיה ומערכות מידע</u>

18.1. על הספק להציג קיומם של התשתיות הטכנולוגיות ומערכות המידע המאפשרות מתן שירות יעיל ואיכותי זמין לרכבת ישראל.

18.2. מערכת זו תבוסס על כלים סטנדרטיים ותעמוד בכל הנדרש בחוק הגנת הפרטיות, התשמ"א – 1981 והתקנות הנגזרות ממנו. כמו כן, תעמוד המערכת בכל הנדרש בתקנות הגנת הפרטיות (תנאי החזקת מידע ושמירתו וסדרי העברת מידע בין גופים ציבוריים), התשמ"ו - 1986 כנדרש למידע רגיש.

18.3. באים יידרש הספק יעמיד מערך גישה מאובטח מרחוק לטובת נציגי רכבת ישראל, הגישה תתבצע ב זיהוי מלא של המשתמשים.

18.4. בהגדרת הרשאות תינתן האפשרות להגבלת כניסה של משתמשי הרכבת לנתוני הרכבת בלבד . לדוגמא נציג יחידה מסוימת יוכל להזמין/לראות את נתוני היחידה שלו בלבד.

18.5. המערכת תשמור את ההיסטוריה של כל הפעולות שבוצעו על כל רשומה ורשומה כולל רשומות שבוערו.

18.6. נציג רכבת ישראל יהיה רשאי בכל עת ובתיאום מראש לבחון את עמידות מערכת המידע ומערכות האבטחה של המציע הזוכה. במקרה של ממצאים ברמת חומרה גבוהה, מתחייב הזוכה לתקנם תוך 14 יום. הפרת התחייבות זו יכולה להביא להפסקת ההתקשרות עם הזוכה.

18.7. בסיס הנתונים של מכלי הרכבת המצוי ברשות המציע הינם רכוש רכבת ישראל בכל תקופת ההתקשרות. בסיום ההתקשרות עם המציע, המציע ימסור את בסיס הנתונים של הרכבת מידית לפי דרישה. המציע יעביר לרכבת ישראל העתק מלא של כלל הרשומות השייכות לה לרבות פירוט התנועות שנעשו בהן. המידע יועבר בקבצים סטנדרטיים (כגון Excel וכדו') לפי מבנה שיסוכם עם רכבת ישראל. לאחר אישור הקבלה על ידי רכבת ישראל וכן ביצוע הקליטה בהצלחה, רשאית רכבת ישראל להורות על מחיקת הקבצים ממערכות הזוכה באופן קבוע.

18.8. הספק ימנה אחראי אבטחת מידע אשר יהיה גורם מנהל\מפקח\מבקר בנושא אבטחת מידע מטעמו, ויהיה גורם מקשר ואחראי מטעם הספק בכל האמור לעיל.

18.9. על המציע לתעד את פרטי יחידת התיוק ופרטי ההפקדות והשליפות של החומר באמצעות מערכת מידע ממוחשבת.

18.10. התיעוד יכלול את המאפיינים שהרכבת תקבע (כמו: שם ומספר יחידה ארגונית, מספר המכל, מועד קבלת המכל, סוג יחידת התיוק, נושא יחידת התיוק, טווח תאריכים, תקופת שמירה, סטאטוס תיק, היסטוריה ועוד)

18.11. המציע יעשה שימוש בכלים המבטיחים שהמידע המסחרי והאישי ינוהל באופן המבטיח שלמות, חיסיון וזמינות הנתונים ושימוש מבוקר בהם, לרבות יישום הגנה של משאבי מערכות המחשב והתקשורת (מתקנים, חומרה, גיבוי, הגנה מפריצות תכנה ונהלים) על הנתונים המאוחסנים בהם.

18.12. על המציע למנוע חשיפת מידע אשר יגרום לרכבת ישראל נזק כלשהוא על ידי גורמים שונים.

18.13. המערכת תהיה מוגנות מפני חדירה בלתי מורשית על ידי שימוש ברכיבי האבטחה מהמובילים בשוק.

18.14. הגישה למערכות תתבצע רק ע"י נציגי רכבת ישראל המורשים ועובדי המציע המאושרים, תוך שימוש בשם משתמש וסיסמה אישית לכל משתמש.

19. <u>ניהול תקשורת ותפעול מערכות מידע של הספק</u>

19.1. אבטחת רשתות

על הספק:

19.1.1. ליישם רבדים של אבטחה בין רשתות שונות של לקוחותיו.

19.1.2. ההפרדה הרשתית תתאפיין הן במישור ניהולי, תפעולי ובקרתי.

19.1.3. ליישם הפרדה רשתית גם על רשתות אשר מכילות נכסים לצורכי חשיפה לנציגי רכבת ישראל לפי הגדרה ולבין כלל הציבור(זאת בהתאם לרגישות הנכסים).

19.1.4. הפרדה רשתית תתבצע במישור לוגי והן ורצוי גם במישור פיזי.

19.1.5. ליישם מערכת בקרה אשר תמנע\תבקר\תפקח על תקלות\התקפות\שיבוש בין רשתות השונות של הספק.

19.1.6. ליישם מערכות הגנה אשר יגנו באופן הולם על מערכות המחשוב, הנתונים, מהימנות הנתונים וזמינות הנתונים.

19.1.7. ליישם מערכת בקרה לזליגת מידע בין רשתות שונות.

19.1.8. מערכת בקרה של הספק תתריע על כל חריגה מהמוזכר בסעיפים קודמים וידווח במידי לממונה אבטחת מידע.

19.2. ניהול רשת

על ההספק:

19.2.1. קישור גורמים חיצוניים מ/אל רשת הספק יתבצע באופן ריכוזי וינוטר בזמן אמת.

19.2.2. לא תאושר כל התחברות "עצמאית", שאינה דרך נקודות כניסה מאובטחות.

19.2.3. ייושם מידור בין החלקים השונים ברשת באמצעות חלוקה לוגית ופיזית של הרשת והגבלת אפשרות הקישור בין הרשתות השונות.

19.2.4. תיושם בקרה וסינון של תקשורת יוצאת ונכנסת על נכסי רכבת ישראל בתיאום עם הספק.

19.2.5. תיושם בקרה על הפעילויות המתבצעות במערכות לאיתור אירועים חריגים בנכסי ר"י. בנוסף לבקרה בדיעבד, תיושם בקרה בזמן אמת.

19.3. בקרת גישה מערכות מחשוב הספק

19.3.1. אכיפת בקרות גישה

19.3.1.1. ייושמו מנגנונים ממוכנים לניהול בקרות גישה במערכות מידע וביישומים (אפליקציות).

19.3.1.2. בקרות גישה יורכבו מאמצעי זיהוי ובקרת הנתיב.

19.3.1.3. מדיניות בקרת גישה תיקח בחשבון מידור מתאים של הרשאות.

19.3.2. אמצעי זיהוי

19.3.2.1. ייקבעו אמצעי זיהוי למערכות ושירותים לצורך זיהוי חד ערכי (Unique User ID) של המשתמש.

19.3.2.2. אמצעי הזיהוי יהיו אישיים ולא יותר שיתוף של אמצעי הזיהוי.

19.3.2.3. אמצעי הזיהוי יוחלו הן על מנהל מערכת מאגף מחשוב ברכבת ישראל והן על משתמשים אחרים (ספקים וכדומה) המתחברים למערכות המחשוב בענן.

19.3.2.4. לכל הפחות, אמצעי הזיהוי יורכבו משילוב של שם משתמש (User Name) וסיסמא.

19.3.2.5. נתוני הזיהוי יישמרו חסויים (הן בתווך התקשורת והן במערכות השונות).

19.3.2.6. ר"י תשקול שימוש באמצעי זיהוי חזק ויעשה שימוש בטכנולוגיה המונעת אפשרות העתקה או שחזור הפריטים.

19.3.2.7. ייקבע פרק זמן של אי פעילות (Session Time Out) באחריות אגף מחשוב, במערכת שלאחריו יופעל מנגנון ניתוק תקשורת שיחייב זיהוי מחדש של המשתמש. במידה ומנגנון הניתוק מטיל מגבלה על פעילות בעלת אופי רציף, יש להתריע לפני ניתוק התקשורת.

19.3.3. ניהול זהויות וגישה

19.3.3.1. על הספק להעביר פרטים מלאים של בעלי תפקידים אשר להם הרשאות לנכסי ר"י.

19.3.3.2. על הספק, ליישם גישה לנכסי ר"י להיעשות באמצעי בקרת גישה מבוססי תפקיד לצורך הקצאת גישה לוגית לפונקציות משרה או לתחומי אחריות ספציפיים

19.3.3.3. גישה לנכסי ר"י תתבצע עם שם משתמש אישי ובאימות של:

19.3.3.3.1. סיסמא - חובה

19.3.3.3.2. מומלץ להכליל גם אסימוני חומרה או כרטיסים חכמים או אמצעים ביומטריים להגברת האימות.

19.3.3.4. השוואה של חשבונות משתמשים אל מול הרשאות לשימוש תתבצע בקביעות על מנת להבטיח ששימוש בנכסי ר"י מתבצע באופן הולם. חשבונות שאין להם עוד צורך בגישה יוגדרו כלא זמינים ויחסמו.

19.3.3.5. כל חריגה משימוש מורשה על ידי חשבונות לא מאושרים תתוחקר, תתבצע פעילות חסימתית וידווח במידית לממונה אבטחת מידע ר"י.

19.3.4. ניהול הרשאות

19.3.4.1. יוגדר תהליך רישום וביטול רישום להרשאות גישה למערכות מידע ולשירותים.

19.3.4.2. ההרשאות יינתנו בהתאם לתפקיד, לפי הצורך לדעת (need to know).

19.3.4.3. חובה לנהל טבלת הרשאות לעובדים בהתאם לתפקידם ולמידע הנדרש להם לצורך ביצוע תפקידם.

19.3.4.4. מתן הרשאות גישה למערכות ושירותים תוגבל ותפוקח בהתאם.

19.3.4.5. ניהול ההרשאות ייעשה ע"י מנגנון ממוכן לניהול הרשאות.

19.3.5. ניהול סיסמאות על ידי הספק

19.3.5.1. הספק יציג מדיניות ניהול סיסמאות לנציג אבטחת מידע ברכבת .

19.3.5.2. הסיסמא תהיה ידועה אך ורק למשתמש.

19.3.5.3. סיסמאות לא ישמרו באופן גלוי (Clear Text) .

19.3.5.4. סיסמא תבוטל מידית בכל מקרה של חשש לפגיעה בחשאיותה. לא יתאפשר לשחזר את הסיסמא.

19.3.5.5. מורכבות הסיסמא, תוקפה ותחולתה לפי סוגי הקהל ייקבעו בתיאום עם נציג רכבת ישראל .

19.3.6. בקרת גישה למערכות ספק

19.3.6.1. בגישה מרחוק לרשת הספק נציגי ר"י, על גבי תשתית תקשורת ציבורית, נתוני ההזדהות למערכת יוגנו ויאובטחו בפני ציתות (הצפנה מקצה לקצה) וזליגת מידע.

19.3.6.2. בגישה למערכות הספק לצורך ביצוע פעולות מהותיות ייעשה שימוש באמצעי זיהוי חזק.

19.3.6.3. הספק יבצע רישום של כל משתמש המקבל גישה דרך רשת ציבורית

20. גיבוי ושחזור

20.1. על הספק לבצע שמירת אמצעי הגיבוי במקום מרוחק, מאובטח ומוגן בפני פגיעה באמצעים ובתוכנם.

20.2. אמצעי הגיבוי ישמרו במקום מרוחק, מאובטח ומוגן בפני פגיעה באמצעים ובתוכנם.

20.3. מדיית הגיבויים ישמרו בכספת חסינת אש.

20.4. הספק יפרסם את תכנית הגיבויים עבור נכסי רכבת.

20.5. טיפול בגיבויים ושחזורים – באחריות הספק .

21. נתיב בקרה וניטור מערכות מחשוב ספק Audit Trail

21.1. הספק יקיים נתיב בקרה לניטור ומעקב אחר ביצוע פעולות ושאילתות .

21.2. תכולת נתיב הבקרה להכיל את הנתונים הרלוונטיים, כך שיתאפשר לגלות ניסיונות גישה ופעולות לא מורשות ולזהות את מקורן. נתיב הבקרה יכלול מידע לפחות על ניסיונות של מורשים ולא מורשים, מוצלחים ולא מוצלחים, מהות הפעולה, מקור הגישה וזמן הגישה.

21.3. יבוצעו בדיקות סדירות של דוחות החיווי והבקרה המתקבלים ממערכות הניטור והמחשוב של החברה.

21.4. כחלק מהבדיקות היומיות תיבדק זמינות המערכת והמשאבים, כולל בדיקת קיבולת המערכת ומגמות השימוש תוך זיהוי "צווארי בקבוק" אפשריים העלולים להוות איום וסכנה על אבטחת המערכת והמידע.

21.5. תהליך הבדיקה היומי יכלול מעקב ובקרה אחר שימוש במשאבי המערכת ו/או שימוש חריג באפשרויות המערכת על ידי משתמשים לא מורשים.

21.6. כל מקרה של חשד ו/או עם כל איתור של ממצא המצביע על אירוע, אשר משפיע או אשר עלול להשפיע על תפקודן של המערכות או על זמינות המידע, אמינותו, חסיונו שלמותו או שרידותו, ידווח הדבר מידית לממונה אבטחת מידע בר"י.

21.7. פרק הזמן לשמירת קבצי התיעוד ייקבע בהתאם להנחיות רכבת ישראל אגף בטחון.

21.8. הספק יבצע מעקבים סדירים אחר אירועים חריגים תוך הצלבת נתונים מאירועים דומים לשם איתור מקור החריגה והאירוע ו/או משתמש נשוא החריגה.

21.9. כל ניסיון גישה כושל וחריג למערכת ינוטר ויתועד במנגנון אירועים.

21.10. יוכן יומן המכיל מידע על תקלות, אירועי אבטחת מידע ופעילויות משתמשים חריגות.

21.11. על שעון מנגנון הניטור להיות מסונכרן עם מקור שעון מדויק לצורך דיוק התיעוד.

21.12. קבצי ה – Log יאובטחו בפני מחיקה, שינוי או קריאה בלתי מורשים.

22. <u>דוחות</u>

22.1. הספק יגיש דוחות במרווחי זמן קבועים בסוגיות הנוגעות באבטחת מידע.

22.2. תדירות הדוחות תקבע בשיתוף עם אגף בטחון ר"י ובהנחייתו.

22.3. רשימת דוחות:

22.3.1. יומן חריגים.

22.3.2. יומן מסירת מידע.

22.3.3. יומן הכנסת מידע.

22.3.4. יומן התחברות מרחוק נציגי רכבת.

22.3.5. יומן שדרוגים ופיתוחים.

22.3.6. דוח הרשאות גישה.

22.3.7. דוח אירועי אבטחת מידע

23. <u>אירועי אבטחת מידע</u>

23.1. <u>ניהול אירועי אבטחת מידע על ידי הספק</u>

23.1.1. הספק ידאג להעמיד צוות אשר ידע ויתפקד באירוע אבטחת מידע

23.1.1.1. **הערכות -** צוות הספק עם מוכנות לתגובתה מידית עם התרחשות אירוע.

23.1.1.2. **זיהוי-** איתור גורם להתרחשות האירוע, בין מדובר באירוע מכוון ובין לאו.

23.1.1.3. **בלימה-** ביצוע פעולות בלימה כדי למזער ולבלום התפשטות אירוע לסביבות אחרות ומזעור הסיכון.

23.1.1.4. **מיתון-** אספקת שירותים רלוונטיים לצמצום הסיכון, ולהישנות האירוע.

23.1.1.5. **שחזור-** ביצוע שיחזור השירות ואו מידע בהתאם לצורך.

23.1.1.6. הפקת לקחים- לאחר פתרון אירוע האבטחה, הערכה, תיעוד והפקת לקחים.

23.1.1.7. הערה- דוח אירוע אשר יכיל את כל הסעיפים הנ"ל כולל תיעוד ביצוע יועבר לרכבת ישראל בקרות אירוע אבטחת מידע באופן מידי.

23.2. <u>מחויבות לשיתוף פעולה באירועי אבטחה מידע</u>

23.2.1. בכל אירוע אבטחת מידע, או שקיים חשד לפגיעה שיש עמה השלכה ישירה או עקיפה על אבטחת מידע ו/או הגנת פרטיות בנוגע לנכסי רכבת ישראל.

23.2.2. בכל הפרה או חשד להפרה של חוקים, תקנות או נהלי אבטחת-מידע.

23.2.3. בחקירת אירועים או חשדות, לחריגות אבטחה.

23.3. <u>ניהול יומן חריגים</u>

23.3.1. הספק מתחייב לנהל דו"חות ומעקב איתור אירועים חריגים בפעולות התמיכה.

23.3.2. הספק, ימציא את יומן האירועים החריגים לנציגי רכבת ישראל, במועד העברת הדרישה.

23.4. <u>הגנה מפני ניסיונות פגיעה</u>

23.4.1. על מנת להגן על מערכות ונכסי רכבת ישראל, הספק ינקוט בכל הצעדים הנדרשים של חשיפה חסימה של ניסיונות פגיעה (כולל איתור, זיהוי ומניעת ניסיונות אלה). אמצעים אלו יגנו מפני שימוש לא תקין במידע, במערכות המידע ובבסיסי הנתונים.

23.4.2. הספק רשאי להשתמש באמצעים מקובלים ונתונים אחרים, ובלבד שמהות אבטחת המידע הנדרשת בסעיף זה לא תפגע.

23.4.3. על הספק להתאים את האמצעים המקובלים והנאותים בהתאם להתפתחויות הטכנולוגיות שישררו באותה עת, ולאיומים ולחשיפות הרלוונטיים לאותה תקופה.

23.4.4. על הספק להכין תוכנית למזעור יכולת פגיעה על ידי עובדי החברה(או נציגה בארץ).

23.4.5. הספק יפרט את אמצעים האבטחתיים אשר ייושמו בכדי להגן על נכסי רכבת ישראל.

23.5. תגובה לאירועי אבטחת מידע

23.5.1. הגדרת אירוע אבטחת מידע

23.5.1.1. אירוע אבטחת מידע שיש לו פגיעה בעלת אופי שיש בו פגיעה בזמינות\אמינות\שרידות\הרשאות נכסי רכבת ומערכותיה יוגדר כאירוע אבטחת מידע חמור.

23.5.1.2. אירוע שקיימת זליגת מידע מנכסי ר"י יוגדר כאירוע אבטחת מידע חמור.

23.5.1.3. אגף בטחון רכבת ישראל בתיאום עם הספק יגדיר את אופן התגובה לאירועי אבטחת מידע למי מדווחים ומהו זמן התגובה הסביר לדיווח.

23.5.1.4. אגף בטחון בר"י יוגדר כפוסק בכל הנושאים הכוללים את קביעת Severity של אירוע.

23.5.2. **דיווח על אירועי אבטחה**

23.5.2.1. במידע ומדובר באירוע בעל אופי שיש בו פגיעה בזמינות\אמינות\שרידות\הרשאות\חסיון וזליגת מידע מנכסי רכבת ידווח ספק במידית לממונה אבטחת מידע.

23.5.2.2. ממונה אבטחת המידע ידווח על פי שיקול דעתו לגורמים נוספים על אירועים חריגים .

23.5.2.3. במקרה ומשתמש בעל הרשאות חושד שמתבצעת פגיעה בנכסי רכבת, עליו לדווח מיד לממונה אבטחת מידע.

23.5.3. תגובה לאירועי אבטחת מידע

23.5.3.1. הספק יפעל במידית לטיפול באירועים אשר פגיעה בזמינות\אמינות\שרידות\הרשאות\חסיון נכסי רכבת ומערכותיה.

23.5.3.2. הספק יעמיד צוות אשר יפעל בהתאם למוזכר בסעיף 23.1.1 במסמך זה.

23.5.4. דיווח על נקודות תורפה

23.5.4.1. אם ידוע על קיומן של פגיעויות בנושא אבטחת המידע ו/או הגנת הפרטיות (אף אם טרם בשלו לכלל אירוע), ידווחו אלו לממונה אבטחת מידע (אגף בטחון ר"י) באופן מידי.

23.5.5. טיפול באירוע אבטחת מידע

23.5.5.1. הספק יעמיד צוות אשר יפעל בהתאם למוזכר בסעיף 23.1.1 במסמך זה.

23.5.5.2. באחריות הספק לבצע חקירה אשר תבדוק את אופי האירוע ותגדיר דרכי תגובה.

23.5.5.3. בעת הצורך, יש לזמן יועצים פנימיים אשר יעזרו להגדיר את האירוע ואת אופי התגובה לאירוע.

23.5.5.4. כל עוד לא ידוע אחרת, קיים צורך להתייחס לאירוע כאל אירוע בעל אופי פגיעה באבטחת מידע ו/או הגנת הפרטיות. על כן יש צורך בתגובה מהירה וחד משמעית.

23.5.6. תיעוד האירוע

23.5.6.1. הספק יתעד את האירוע. תיעוד זה יתבצע באמצעות שמירת קבצים רלוונטיים, צילומי מסך ועוד.

23.5.6.2. ינוהל יומן אירועים לתיעוד האירוע.

23.5.6.3. לאחר סיום האירוע הספק יכתוב דוח המתעד את אירוע אבטחת המידע ואת הראיות שנאספו במהלכו ומתעד את הפעילות שבוצעה בנידון. העתק הדוח והראיות יומצאו תוך 48 שעות מזמן סיום האירוע לר"י.

23.5.7. הפקת לקחים מתקריות

23.5.7.1. הספק יקיים פגישות עבודה עם גורמים רלוונטיים על מנת להפיק לקחים.

23.5.7.2. הספק יבצע הפקת לקחים ויתווה תכנית לטיפול בממצאים תוך דיווח התקדמות התוכנית לר"י –לאגף רלוונטי .

24. <u>ראיות ועדי הספק</u>

24.1. הספק יתחייב להמציא לר"י כל ראיה (דיגיטלית, כתובה או אחרת) תוך 48 שעות מזמן הבקשה.

24.2. הספק יתחייב הוא ועובדיו ישתפו פעולה עם גורמי חוק וביטחון במדינת ישראל, ובכלל זה יתייצבו למתן עדות במועדים אשר ר"י ו\או גורמי החוק והביטחון במדינת ישראל יקבעו.

25. <u>אבטחת מידע ב שירותים שוטפים</u>

25.1. הכנת החומר למשלוח באתרי ר"י

25.1.1. כל חומר ארכיוני באתר הרכבת הנועד למשלוח ייארז באריזה נפרדת.

25.1.2. האריזה תיסגר הרמטית ותפתח אך ורק עם הגעתה ליעד אתר הארכיון.

25.1.3. פתיחת האריזה תתבצע לאחר בדיקה שלא נפתחה בדרך ותתבצע על ידי מי שהוסמך לכך.

25.1.4. סימון האריזה יהיה ייחודי לרכבת ישראל.

25.1.5. על הדופן החיצונית של המכל יש לרשום את שם היחידה ארגונית/האתר, מספר היחידה .

25.2. <u>הובלת החומר לארכיב</u>

25.2.1. המציע מתחייב להעביר את כל הארגזים שהועמסו בשלמותם לארכיב, כאשר החומר ארוז במכלים סגורים ולאחר שווידא, טרם העמסתם באתר האיסוף, כי האריזה לא נפגמה.

25.2.2. הובלת חומר השייך לרכבת תתבצע בהפרדה מוחלטת מחומרים בעלי שייכות אחרת.

25.2.3. העברה תתבצע בכלי רכב של המציע שיאושרו ע"י רכבת ישראל. רכב סגור הכולל נהג ומלווה, לא יישאר רכב ללא השגחה כאשר יש בו ארגזים של הרכבת.

25.2.4. רכב של המציע, במידה ויש עליו מכלים של הרכבת, לא יחנה בלילה מחוץ לחצרות המציע.

25.2.5. הובלת החומר תיעשה ברכב בעל תא מטען סגור בלבד, אשר ייסע ישירות לבית הארכיב לאחר איסוף החומר.

25.3. <u>קליטה ומפתוח של החומר בבית הארכיב</u>

25.3.1. לפני תחילת כל פעילות על מכלים של הרכבת יוגדרו על ידי הרכבת, בתאום הספק הזוכה, קודי היחידות, שמותיהם, סוגי החומר השונים ותקופות שמירה

לכל סוג חומר. הגדרה זו תתבצע על ידי נציג הרכבת אשר אחראי על התקשרות זו. כל שינוי ו/או תוספת תדרוש אישור שלו, שינויים בהגדרות אלה לא יתבצעו על ידי נציגי היחידות. ללא הגדרה זו לא תתקיים כל פעולה על מכלי הרכבת כולל העברת הארכיב הקיים.

25.3.2. מיד עם הגעת המשאית לחצרות המציע יש לבצע בקרת שלמות של כל משלוח ומשלוח. בקרת השלמות תתבצע על פי תכולת תעודת המשלוח שהוכנה עם העמסת המכלים באתר/יחידה ארגונית למול המלאי שנתקבל בחצרות המציע.

25.3.3. לאחר ביצוע בקרת השלמות יש להודיע לנציג הרכבת ולנציג היחידה השולחת שכל המכלים נתקבלו בחצרות הספק.

25.3.4. במידה ובבקרת השלמות נמצאה אי התאמה, יש לעצור מידית כל פעילות על המשלוח ולפנות לנציג הרכבת ולנציג היחידה השולחת ולקבל הנחיות בכתב.

25.3.5. עם פריקת החומר בארכיב, על המציע לבצע בדיקת תקינות המכלים. במידה וישנה פגיעה באריזה יש להחליף מיכל ולהעביר אליו את כל מאפייני הזיהוי שהיו על המכל לפני שניזוק.

25.3.6. אין להשאיר את החומר לאחר פריקתו בשטח לא מקורה מחוץ לגבולות מבנה הארכיב.

25.3.7. המציע יקלוט את פרטי המכלים ופרטי תכולתם התיקים/מעטפות/קלסרים אשר במכלים במערכת המידע הממוחשבת עפ"י השדות המוגדרים ע"י רכבת ישראל.