13-11-2016

נספח אבטחת מידע לחוזה – ספק מערכת מחשב

1. מטרת המסמך

1.1. להוות נספח אבטחת מידע לחוזה עם ספק מערכת/ציוד מחשב לרכבת.

1.2. מסמך אשר יתייחס להיבטי אבטחת מידע אשר על הספק ליישמם בהתקשרות עם רכבת ישראל.

1.3. נספח אבטחת מידע זה יצורף למכרז, בהתאם לרכש תכולתו.

2. כללי

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

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

2.3. פגיעה במידע, במאגריו או במערכותיו, 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.

2.4. היות וברכבת ישראל מתקיימים מכרזים מסוגים שונים ,אין לראות נספח זה מכיל ומקיף את כלל המכרזים.

2.5. בהתאם לתכולת המכרז יוסף נספח אבטחת המידע שיותאם אליו.

3. הגדרות

3.1. **ר"י**-רכבת ישראל

3.2. **ספק** - חברה אשר מתמודדת במכרז ומספקת שירותים, טובין, יעוץ לרכבת ישראל.

3.3. **יועץ** - חברה המספקת שירותי יעוץ לר"י על ידי עובדיה או מי מטעמה.

3.4. **נכס ר"י** - מידע, אפליקציה, מערכות, ממשקים השייכים לר"י.

3.5. **המכרז** – מכרז לקבלת טובין ,שירותי יעוץ, אספקת ותחזוקת מערכות מחשוב בר"י .

3.6. **מידע** - כל מידע (Information), ידיעה, מסמך, תכתובת, תכנית, נתון, מודל, חוות דעת, מסקנה וכל דבר אחר כיו"ב הקשור ו/או הנוגע למתן השירותים, לרבות מידע הנוגע לצנעת הפרט של עובדי החברה ,בין בכתב ובין בע"פ ו/או בכל צורה או דרך של שימור ידיעות בצורה חשמלית ו/או אלקטרונית ו/או אופטית ו/או מגנטית ו/או אחרת, הקשורים ו/או הנוגעים למתן השירותים, אשר אינו מצוי בנחלת הכלל.

טל 04-856-4177 **פקס** 04-856-4363 **נייד** 050-792-2059 **E-Mail: ilanf@rail.co.il**

3.7. **סודות מקצועיים** - כל מידע אודות הרכבת אשר יגיע לידי היועץ או עובד מטעמו בקשר למתן השירותים, בין אם נתקבל במהלך מתן השירותים או לאחר מכן, לרבות ומבלי לפגוע בכלליות האמור לעיל: מידע אשר יימסר ע"י המזמין ו/או כל גורם אחר ו/או מי מטעמו.

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

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

3.10. **גניבת זהות**- ניסיון לגניבת זהות או מידע אישי ע"י התחזות לגורם רשמי המבקש מידע זה .

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

3.12. **הצפנה** - יישום של קריפטוגרפיה הממירה מידע גלוי (Clear Text) למידע מקודד (Cipher Text) באופן שיוכל להיות מפוענח ומובן אך ורק לגורמים מורשים.

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

3.14. **חשיפה** – Vulnerability- חולשה במערכת העלולה להוביל להתממשות איום.

3.15. **לוג** – **Log** - קובץ התיעוד של נתיב בקרה.

3.16. **מידע רגיש** - מידע שר"י סיווגה כבעל סיווג הדורש אמצעי אבטחת מידע נאותים כדי שיהיה נגיש רק למורשים.

3.17. **מערכות מידע** - כלל הציוד הממוכן התומך בעיבוד והצגת מידע של ההחברה הכולל בין השאר: שרתים, מחשבים נייחים וניידים, ציוד תקשורת, ציוד אבטחת מידע ועוד.

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

3.19. **רמו"ט** – רשות מידע וטכנולוגיה במשרד המשפטים, האחראית לנושא הגנת הפרטיות ורישום מאגרי מידע.

3.20. **סקר סיכונים** - סקר המאתר איומים/חשיפות ,הקשורות באבטחת מידע במערכות שונות, ומעריך את רמת הסיכון שלהם לרכבת ישראל .

4. התקשרות עם ספק

4.1.סוגיות משפטיות מול הספק

4.1.1. ר"י תפנה את הטיפול בנושא למחלקה המשפטית ברכבת.

4.2.חוקי המדינה

טל 04-856-4177 פקס 04-856-4363 נייד 050-792-2059 E-Mail: ilanf@rail.co.il

4.2.1. ספק השירותים/מערכת ימלא במלואן את ההוראות והחוקים במדינת ישראל כדוגמת:

4.2.2. חוק המחשבים.

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

4.2.4. חוקי דיני ראיות.

4.2.5. כל חיקוק עתידי לניהול מאגרי מידע ולשמירתם.

4.2.6. הנחיות גופים מנחים את הרכבת.

4.2.7. כל בירור והתדיינות בסוגיות משפטיות 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.

4.2.8. הסעיפים הנ"ל יוכנסו בחוזה שיחתם בין רכבת ישראל לספק.

4.3.חוזה

4.3.1. הספק יתחייב שלא למסור/להעביר מידע אשר יימצאו במערכותיו והינו שייך לרכבת ישראל – ללא אישור בכתב ומראש מהרכבת.

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

4.3.3. החוזה ינוסח בצורה אשר תחייב לנקוט בכל הצעדים הנדרשים לשם הגנה על המידע.

4.3.4. בחוזה ייקבעו בין השאר:

4.3.4.1. אמצעי אבטחת מידע והגנת פרטיות.

4.3.4.2. גיבוי.

4.3.4.3. המשכיות עסקית.

4.3.4.4. אמנת שירות.

4.3.4.5. סיום התקשרות.

4.3.4.6. אחריות הספק לשמירת זמינות המידע, אמינותו, חסיונו, שלמותו של ר"י.

4.3.4.7. סקרים תקופתיים ובקרות

4.3.4.8. זכויות חוזיות.

4.3.4.9. איסוף ראיות דיגיטליות וזימון עובדי הספק לעדות, אם הדבר יידרש

4.3.4.10. ממשקים בין הספק לבין מערכות ר"י.

4.4.סיום ההתקשרות

4.4.1. הספק מתחייב להעביר את כל המידע לרכבת ישראל או לספק אחר מטעמה.

4.4.2. הספק מתחייב להשמיד כל מידע השייך לרכבת ישראל המצוי ברשותו ואשר לא יימסר לרכבת.

אילן פריש – ממונה אבטחת מידע

טל 04-856-4177 **פקס** 04-856-4363 **נייד** 050-792-2059

E-Mail: ilanf@rail.co.il

4.4.3. בעת סיום התקשרות עם ספק השירות יש לוודא שהדיסקים הקשיחים אשר הכילו מידע של הארגון נמחקים בהתאם לנוהל FIPS SP 800-88 - Guidelines for Media Sanitation, כאשר יש להתייחס לכל פריט מידע כ"מידע רגיש".

4.5.פרטיות

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

4.5.2. הספק יתחייב לעמוד בהתאם לחוק הגנת פרטיות ותקנות העזר, ובכלל זה נהלי רמו"ט.

4.5.3. כל שינוי במדיניות הספק בנוגע להגנת הפרטיות יובא לאישור ר"י.

4.6.חוקיות התכנה ופלטפורמת מחשוב

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

4.7.זכויות חוזיות

4.7.1. בהתאם לזכויות החוזיות, רשאית רכבת ישראל:

4.7.1.1. לדרוש דוח על ליקוי אבטחה ו/או ליקויים בתחום הגנת הפרטיות, במידה וקיים חשד ברכבת ישראל על קיומם.

4.7.1.2. להורות לחברה להפסיק העסקתו של עובד זה או אחר, מטעמים הנוגעים לביטחון מערכות המחשוב ומאגרי המידע , המשמשים את רכבת ישראל.

4.7.1.3. 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). במקרה של ליקויים קריטיים, תידרש החברה לתקן ליקויים אלו באורח מידי.

4.8.הצהרת סודיות

4.8.1. 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.

4.8.2. כל טפסי הצהרת הסודיות יועברו לרכבת ישראל.

4.9.קניין

4.9.1. כל המידע, התוכנות, האפליקציות, הנתונים, קוד וכו' אשר יאוחסנו בענן מחשבי יהיו בבעלותה המלאה והבלעדית של ר"י.

4.9.2. הספק יצהיר כי הוא מוותר על זכותו לתבוע כל זכות קניינית מר"י , ובכלל זה את הזכות לקניין רוחני.

4.10. אמנת שירות

טל 04-856-4177 **פקס** 04-856-4363 **נייד** 050-792-2059
E-Mail: ilanf@rail.co.il

4.10.1. ר"י תקבע אמנת שירות עם הספק אשר תתבסס על זמינות, אמינות וסודיות מידע (נכסי רכבת).

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

4.11. מסירת מידע והסכם חסיון

4.11.1. הספק לא ימסור מידע ממאגרי המידע, ומידע על אבטחת המערכות נשוא ההתקשרות זו לשום גוף או אדם, ללא אישור בכתב מאגף בטחון או מי מטעמו (ממונה אבטחת מידע).

4.11.2. 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.

4.11.3. 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.

5. מכרז לאספקת מערכת

5.1. על המערכת המסופקת לקיים עקרונות אבטחת מידע כלליים כמו:

5.1.1. קיום מנגנונים מפותחים של זיהוי, אימות והרשאות.

5.1.2. מערכת ההרשאות תפעל על פי העיקרון: "הכול אסור אלא אם כן הוגדר אחרת" (Default Deny Stance).

5.1.3. המערכת תקל ככל האפשר על תחזוקתה, ניהול ההרשאות, המשתמשים שלה וכו' .

5.1.4. המערכת תהיה גמישה ככל הניתן, תאפשר שינוי ברירות מחדל, ופרמטרים.

5.1.5. המערכת תהיה נוחה להתממשקות למערכות חיצוניות לצורך יצוא ויבוא נתונים.

5.1.6. המערכת תספק שירותי ניטור, דיווח ופיקוח נאותים.

5.2. יכולות זיהוי ואימות (identification and authentication)

5.2.1. על הספר לפרט

5.2.1.1. יכולות זיהוי משתמשים במערכת, וכן לבצע אימות שאכן מדובר במשתמש שהזדהה. תהליך זה מתרחש בשלב הראשוני של הכניסה למערכת, לפני שהמשתמש קיבל הרשאות כלשהן למשאבי המערכת. על המשתמש לספק מידע אשר יוכיח את זהותו.

5.2.1.2. המנגנון לזיהוי ואימות משתמשים(גם במהלך (session.

5.2.2. **מדיניות סיסמאות**.

5.2.2.1. פירוט כלי המערכת לקביעה ואכיפה של מדיניות סיסמאות מרכזית, לגבי (לפחות) איכות הסיסמא (אורך, תווים חוזרים,

תווים עוקבים, QWERTY וכו'), תוקף, ניסיונות גישה כושלים ונעילות ו History-.

5.2.2.2. היכולת לשנות את הסיסמא.

5.2.2.3. המערכת תאפשר לקבוע אילוץ החלפת סיסמא תקופתית.

5.2.2.4. הסיסמא לא תעבור גלויה ברשת.

5.2.3. ייחודיות קבוצות, תיבות, קבוצות משתמשים, מסמכים, תכניות , קבצים וכו' .

5.2.4. יכולת קישוריות לשרתים חיצוניים של זיהוי ואימות לדוגמא:

5.2.4.1. הסתמכות על הזדהות מול מערכת ההפעלה (לדוגמא באמצעות שירותי Active Directory – קרברוס) .

5.2.4.2. התממשקות לשרת Directory מרכזי (LDAP/DAP)

5.2.4.3. התממשקות למנגנוני הזדהות של סיסמא חד פעמית, או כרטיסים חכמים (RADIUS, וכו').

5.2.5. פירוט האם ההסתמכות הינה חד-כיוונית, והאם הרשאות באפליקציה הינן מקור לאסקלציה של הרשאות בפלטפורמות "נמוכות" יותר?

5.2.6. פירוט האם מתבצע באפליקציה ו/או בתוכניות זיהוי hard coded?

5.2.7. פירוט האם כל המשתמשים יהיו ניתנים למחיקה, וכל הסיסמאות ניתנות לשינוי תקופתי.

5.2.8. פירוט על מנגנון הזיהוי והאימות להתממשק למנגנון ה-audit אשר יתואר בהמשך.

5.3.מנגנון הרשאות

5.3.1. הענקת הרשאות הגישה במערכות השונות תתבסס על שיטת ה- DAC (Discretionary Access Control). בשיטה זו יוגדרו הרשאות ספציפיות לאובייקטים במערכת על-פי שמות המשתמשים, שמות קבוצות משתמשים או שניהם יחד. שינוי הרשאות הגישה יתבצע על-ידי גורמים מוסמכים בלבד.

5.3.2. על הספק לפרט את מנגנון ההרשאות של המערכת.

5.3.3. יש לפרט יכולת ניהול הרשאות: ברמת המשתמש, ברמת קבוצת משתמשים, ברמת סוג המידע, ברמת אובייקט (מסך, כפתור, רשומה, שדה), ברמת קבוצות אובייקטים, וכו' .

5.3.4. יש לפרט יכולת קביעת הרשאות מגוונת (read, write, update, delete) ולא רק access, deny access)).

5.3.5. הספק יפרט קיום אפשרות קביעת פרופיל משתמש לכל קבוצה או תפקיד ארגוני ומתן אפשרות לניהול נוח של מערך פרופיל המשתמש. פרופיל המשתמש לא יהיו חשבונות משתמש לגיטימיים במערכת אלא ישמשו להקניית הרשאות בלבד.

אילן פריש – ממונה אבטחת מידע
טל 04-856-4177 פקס 04-856-4363 נייד 050-792-2059
E-Mail: ilanf@rail.co.il

5.3.6. יש לפרט אמצעי חלחול ההרשאות שבמערכת (האם שיוך משתמש לקבוצת משתמשים יעביר אליו גם את ההרשאות של הקבוצה, שינוי פרופיל הרשאות ישנה הרשאות לכל מי שמשויך לפרופיל זה, וכו').

5.3.7. יש לפרט גמישות ניהול הרשאות.

5.3.8. יש לפרט יכולות תמיכה במנגנוני הרשאות חיצוניים.

5.4.ניהול משתמשים

5.4.1. חלק קריטי ועיקרי מכל יישום ומערכת הרשאות, הינו מודול ניהול המשתמשים שלו. על הספק להציע מנגנון ניהול הקמת ותחזוקת משתמשים גמיש, ידידותי ונוח.

5.4.2. הספק יפרט את :

5.4.2.1. מנגנוני ניהול המשתמשים של המערכת.

5.4.2.2. תמיכת מערכת ביצירת מבנה הירארכי חכם במערכת ההרשאות, והיכולת לחברו לתוכן הרלוונטי בתוך האפליקציה (מאפשר תחזוקה אוטומטית של משתמשים, עפ"י מקומם ההירארכי).

5.4.2.3. אפשור ניהול חכם של קבוצות (קבוצה בתוך קבוצה, קבוצות חופפות וכו').

5.4.2.4. אפשור יצירת משתמש ע"י העתקת משתמש קיים, או ע"י העתקת פרופיל משתמש.

5.4.2.5. אפשור מחיקת משתמשים מהמערכת.

5.4.2.6. מערכת דוחות גמישה, כמפורט בסעיף הבא.

5.4.2.7. אפשור קליטת משתמשים חדשים וביטול משתמשים בצורה גורפת (Batch).

5.4.2.8. יכולות התממשקות למערכות חיצוניות של ניהול משתמשים. יש לפרט ממשקים מוצעים מול מערכות חיצוניות אשר יאפשרו הפעלת פונקציות (הקמת משתמש, מחיקה, שינוי הרשאות) למשל, בעזרת API או בעזרת פקודות prompt.

5.5.**תיעוד, בקרה והתראה** (log, audit and alert)

5.5.1. מערכת תשלב פתרון לתעד פעילות אשר תוגדר קריטית במערכת, פעילות אשר נראית חריגה (כולל פעילות בבסיס הנתונים ו/או במערכת ההפעלה), ופעילות או ניסיונות לביצוע פעולות אשר נוגדת ישירות policies כפי שהוגדרו במערכת. כמו כן, על המערכת לספק כלים מתאימים לשמירה על קבצים אלו ויכולות דיווח לבעלי התפקידים המתאימים כדי שיוכלו לטפל בהתרעות.

5.5.2. מנגנון הבקרה (Audit) במערכות יאפשר ביצוע מעקב אחר האירועים הבאים :

5.5.2.1. שימוש במנגנון ההזדהות (login/logout, ניסיונות כושלים, וכו').

5.5.2.2. ניסיון כושל בכניסה למערכת.

5.5.2.3. ניסיונות גישה למידע שאין לו הרשאת גישה.

5.5.2.4. אירועים אפליקטיביים שיוגדרו כדורשי בקרה עפ"י מנגנון כללים מיוחד לנושא.

5.5.2.5. התחלת פעילות מסוימת אשר תוגדר כדורשת בקרה על-ידי המשתמש (פתיחת כספת, שליחת מסר וכו').

5.5.2.6. מחיקת אובייקטים במערכת.

5.5.2.7. פעילויות המבוצעות על-ידי גורמים בעלי הרשאות גבוהות.

5.5.2.8. פעולות אדמיניסטרציה (ניהול משתמשים, הורדה והעלאת מערכת, services, וכו').

5.5.2.9. שגיאות תפעוליות (נפילת מערכת, הודעות שגיאות תוכנה, וכו').

5.5.2.10. עבור כל אירוע המוגדר כדורש בקרה יישמרו הפרטים הבאים:

5.5.2.10.1. תאריך ושעה.

5.5.2.10.2. מקור ביצוע הפעולה (דוגמא: כתובת IP, domain)

5.5.2.10.3. שם המשתמש.

5.5.2.10.4. סוג האירוע.

5.5.2.10.5. הצלחה או כישלון של האירוע.

5.5.2.10.6. זיהוי האובייקט עליו מבוצעת הפעולה (דוגמא: שם קובץ).

5.5.2.10.7. תיאור הפעולה (מה בוצע): עבור כל סוג אירוע יש לספק תוכן רלוונטי. למשל: עדכון רשומה, ניסיון גישה לרשומה, מחיקת משתמש, הורדת מערכת, וכו' .

5.5.3. על ההודעות צריכות להיות אמינות, מלאות וברורות.

5.5.4. על הספק לפרט יכולות המערכת לייצא את הנתונים לקונסולה מרכזית (מערכת שו"ב).

5.5.5. על מנגנון הבקרה להתממשק למנגנון הדוחות ולספק רמה גבוהה של דוחות, חיתוך מידע, וכו' .

5.5.6. על הספק לפרט יכולות דיווח של המערכת (במייל, SMS, snmp traps וכו') למנהלי המערכת על אירועים שיוגדרו כדורשי דיווח.

5.5.7. על מערך הבקרה להיות מאובטח כיאות. רק משתמשים מורשים יקבלו גישה אליו, ובמיוחד יש להקפיד על בקרת גישה ליכולת להעלות ולהוריד את מנגנון הבקרה.

5.6.מערכת דוחות

טל 04-856-4177 פקס 04-856-4363 נייד 050-792-2059

E-Mail: ilanf@rail.co.il

5.6.1. על הספק לפרט בנוגע למערכת דוחות גמישה על המנגנונים הבאים:

5.6.2. דוחות על מערכת ההרשאות (הרשאות למשתמש, משתמשים בקבוצת משתמשים, וכו').

5.6.3. דוחות ממערכת ה-auditing (מספר אירועים מכל סוג, ניסיונות גישה כושלים, וכו').

5.6.4. יכולת יצוא של הקבצים לתוכנות חיצוניות (פורמט XML, DOC, TXT, וכו').

5.6.5. קיום banner המסווג את הדוח, מציין את שם המשתמש שהפיק אותו, תאריך ושעה.

5.6.6. על מערכת הדוחות לאפשור למנהל המערכת להגדיר דוחות חדשים.

5.6.7. על הדוחות להיות קריאים, ברורים ואמינים.

5.7. מניעת התכחשות (Non Repudiation)

5.7.1. על הספק לפרט תמיכה במנגנוני מניעת התכחשות באמצעות חתימה דיגיטאלית על המסרים (בהתאם לחוק החתימה האלקטרונית הישראלי).

5.8. ניתוח פרוטוקולים

5.8.1. על הספק לפרט את הפרוטוקולים המשמשים את האפליקציה בממשק עם תוכנת הלקוח, בזמן ביצוע הזדהות, בממשקים עם בסיס הנתונים, ועם שרתים ומודולים חיצוניים אחרים. על הספק לפרט את אמצעי אבטחת המידע שבפרוטוקולים אלו.

5.9. שלמות הנתונים

5.9.1. במקרים רבים יש לדאוג לכך שיחסים בין נתונים שונים במערכת יישמרו, שמידע לא ייפגם כתוצאה מתהליכי עיבוד ועדכון ממושכים, ושתהליכים יוכלו להיות "משוחזרים". כמו כן, מנגנונים מתאימים צריכים להבטיח שלמות נתונים בעת העברת נתונים בין מערכות, בין משתמשים, או בין אובייקטים במערכת.

5.9.2. על הספק לפרט מנגנונים הקיימים לשלמות נתונים .

5.9.3. על הספק לפרט קיום מנגנוני בדיקה לתהליכי עדכון מסיביים במערכת, השוואה עם גיבוי שלפני הפעולה, הצלבת תוצאות, וכו'.

5.9.4. על הספק לפרט קיום תהליך ניהול תהליכים אשר יאפשר יכולת שיחזור וטיפול של רשומות שסנכרונן נכשל.

5.9.5. על הספק לפרט הפעלת פרוטוקולים של שלמות על נתונים המועברים בין יישומים, ייצוא ויבוא של נתונים. קיום מנגנון מעקב וטיפול בתקלות בחילופי מידע בין מערכות (ראה גם סעיף העברת נתונים בהמשך).

5.9.6. על הספק לפרט קיום מנגנוני אחזור נתונים במקרה של תקלה, שגיאה או מעבר למערכת גיבוי.

אילן פריש – ממונה אבטחת מידע

טל 04-856-4177 פקס 04-856-4363 נייד 050-792-2059

E-Mail: ilanf@rail.co.il

5.9.7. על הספק לפרט קיום מנגנוני שלמות נתונים בבסיס הנתונים (למשל, קביעת יחסים בין שדות, referential integrity).

5.10. זמינות

5.10.1. על הספק לפרט אילו מנגנונים יושמו בכדי לשמר זמינות הנתונים.

5.11. סודיות ופרטיות

5.11.1. על הספק לפרט תמיכה בסיווג המידע ובשמירה על חסיון הפרט. פירוט ל:

5.11.2. תמיכה בסוגי מידע שונים(מידע רגיש וכ').

5.11.3. יכולת ציון במערך ההרשאות של מסכים/קבצים/שדות או כל אובייקט אחר כרגיש. על כן, יהיו מסכים אשר לא יוצג בהם מידע רגיש, או מידע אישי למשתמשים מסוימים. לחילופין, יש להגדיר במידת הצורך מסכים נפרדים: אחד הכולל את המידע הרגיש ואחד שלא.

5.11.4. יכולת הגדרה במערכי ה-audit לרישום גישה או ניסיונות גישה למידע המוגדר כרגיש.

5.11.5. יכולת סימון רגישות המידע על דוחות המערכת.

5.11.6. מניעת אפשרות לבקשות לאחזור מידע כלליות, אלא רק בעלת קריטריונים ספציפיים.

5.11.7. יכולת לעצב תהליכים אשר דורשים אישור של יותר מבן-אדם אחד (עקרון חשב-מבקר).

5.11.8. יכולת לערבל (scramble) נתונים המועברים מסביבת ה-production לסביבות אחרות (ראה גם סעיף הפרדה בין סביבות).

5.12. הצפנה

5.12.1. על הספק לפרט לגבי שיטות ההצפנה שבשימוש המערכת:

5.12.1.1. תהליך ורכיבי ההצפנה (מסמכים, מסרים, כספות, בסיס נתונים, ממשקים וכו').

5.12.1.2. פרוטוקולים (כגון: DES, AES, SSL3).

5.12.1.3. תהליכי ניהול מפתחות במערכת.

5.12.1.4. הצפנת קובצי הסיסמאות.

5.12.1.5. הצפנה של המידע העובר ברשת (מול המשתמש ומול מערכות אחרות)

5.12.1.6. הצפנת נתונים המועברים בין יישומים.

5.13. הפרדת סביבות

טל 04-856-4177 פקס 04-856-4363 נייד 050-792-2059 E-Mail: ilanf@rail.co.il

5.13.1. על הספק לפרט את יכולות המערכת המוצעת לעבוד עם סביבות שונות (test ,QA, production, development, staging).

5.13.2. יש לפרט מערך הרשאות והזדהות נפרד לכל סביבה.

5.13.3. יש לפרט יכולות העברת מידע מאובטחת מסביבה לסביבה, כולל תמיכה ב-workflows מתאימים לנושא אם יש.

5.13.4. כמו כן יש לפרט:

5.13.4.1. יכולות העברה מפיתוח לייצור כך שבמהלך התהליך לא תיפגענה זמינות ושלמות נתוני הייצור.

5.13.4.2. בעת העברת המידע מסביבת הפיתוח לסביבת הייצור, מעבר ההרשאות יהיה אופציונלי, כלומר – יש לאפשר את שתי האופציות: להעביר את מערך המשתמשים וההרשאות, ולא להעבירם.

5.13.4.3. האם קיימת יכולת scrambling לנתונים רגישים במעבר מסביבת הייצור לסביבות אחרות כדי שלא יופיעו בסביבות הלא מבצעיות (Test, QA, וכו') "as is".

5.14. **העברת מידע** (data transmission)

5.14.1. העברת מידע בין ר"י לשאר עולם, ממשקים עם מערכות אחרות, קשר רציף המעדכן מאגרי מידע במקומות שונים, כל אלו הינם מקור לפרצות אבטחת מידע שונות. על הספק לפרט מנגנונים הקיימים למטרות אלו בשידור מידע או העברתו בין אפליקציות בתחומים הבאים:

5.14.2. זיהוי ואימות (Authentication)

5.14.3. בקרת גישה (Access control)

5.14.4. סודיות (Data confidentiality)

5.14.5. שלמות (Data integrity)

5.14.6. מניעת התכחשות (non-repudiation)

5.15. ניהול session

5.15.1. על המערכת לספק פונקציות ניהול session מפותחות על מנת לשמור על יכולת non-repudiation ועל בטחון ה-session (כ- session ניתן להגדיר את מכלול הפעולות אשר המשתמש מבצע מעת ההזדהות וכניסתו למערכת, ועד ליציאה).

5.15.2. על הספק לפרט את מנגנון ניהול ה- session שבמערכת המוצעת.

טל 04-856-4177 פקס 04-856-4363 נייד 050-792-2059
E-Mail: ilanf@rail.co.il

5.15.3. יש לפרט אילו כלים מתאימים לספק לזיהוי וקיום ה-session בצורה מאובטחת, במטרה למנוע התקפות מסוג session hijacking, ו-man in the middle attacks.

5.15.4. יש לפרט אמצעים להצפנה של הקשר אם קיימים, כדי למנוע האזנה ל-session בין הלקוח לשרת.

5.15.5. יש לספק אמצעים ל-end-to-end identification דרך כל ה-session, גם אם "עובר" דרך שרתים ומודולים שונים, לצורכי היכולת לתיעוד תהליך, ושמירה על עקרון ה- non-repudiation, וכן גם כדי למנוע התקפות כדוגמת אלו בסעיפים קודמים.

5.16. אירועי אבטחת מידע

5.16.1. ניהול אירועי אבטחת מידע על ידי הספק:

5.16.1.1. הספק יפרט דרכי ניהול באירועי אבטחת מידע בהתייחסות ל:

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

5.16.1.1.2. **זיהוי** - איתור גורם להתרחשות האירוע, בין מדובר באירוע מכוון ובין לא.

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

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

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

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

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

5.16.2. הספק יפרט מחויבותו לשיתוף פעולה באירועי אבטחה בתחומים:

5.16.2.1. 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.

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

5.16.2.3. בחקירת אירועים או חשדות לחריגות אבטחה.

5.16.3. הספק יפרט אופן ניהול יומן חריגים:

5.16.3.1. דו"חות ומעקב איתור אירועים חריגים בפעולות התמיכה.

טל 04-856-4177 פקס 04-856-4363 נייד 050-792-2059
E-Mail: ilanf@rail.co.il

5.16.3.2. יומן האירועים החריגים לנציגי רכבת ישראל, במועד העברת הדרישה.

5.16.4. הגנה מפני ניסיונות פגיעה

5.16.4.1. הספק יפרט את אמצעי האבטחה אשר יושמו בכדי להגן על נכסי רכבת ישראל.

5.16.4.2. על הספק לפרט תכנית למזעור יכולת פגיעה על ידי עובדי החברה (או נציגה בארץ).

5.16.5. תגובה לאירועי אבטחת מידע

5.16.5.1. הגדרת אירוע אבטחת מידע.

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

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

5.16.6. דיווח על אירועי אבטחה

5.16.6.1. במידע ומדובר באירוע בעל אופי שיש בו פגיעה זמינות/אמינות/שרידות/הרשאות/חסיון וזליגת מידע מנכסי רכבת ומערכותיה ידווח ספק במידית לממונה אבטחת מידע.

5.16.7. תגובה וטיפול לאירועי אבטחת מידע

5.16.7.1. הספק יפרט אופן טיפולו בתגובה לאירוע .

5.16.7.2. למען הסר ספק אגף הביטחון בר"י יוגדר כפוסק בכל הנושאים הכוללים את קביעת Severity של אירוע.

5.16.8. תיעוד האירוע

5.16.8.1. הספק יפרט את נושא תיעוד האירוע.

5.16.8.2. תיעוד זה יתבצע יכלול:

5.16.8.2.1. שמירת קבצים רלוונטיים, צילומי מסך ועוד.

5.16.8.2.2. ניהול יומן אירועים לתיעוד האירוע.

5.16.8.2.3. כתיבת דוח בסיום אירוע 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.

5.17. תיעוד

5.17.1. יישמר תיעוד לגבי תפיסת האבטחה הכוללת של המערכת, מנגנוני האבטחה השונים המיושמים בכל מערכת ותוצאות הבדיקות שנעשו לבחינת יעילות מנגנוני האבטחה. על בסיס עקרונות אלה יבצע הספק אפיון מפורט של מערך אבטחת המידע במערכת המוצעת וכן אפיון כל מערך ההרשאות ע"פ קבוצות משתמש.

5.18. שלמות קוד המקור

טל 04-856-4177 פקס 04-856-4363 נייד 050-792-2059

E-Mail: ilanf@rail.co.il

5.18.1. על הספק להתחייב כי:

5.18.1.1. קוד התוכנה מכיל רק את מה שנרשם בתיעוד המסופק עם התוכנה וסוכם מול תהיל"ה.

5.18.1.2. קוד התוכנה חופשי מסיסמאות ניהול, דלתות אחוריות, סוסים טרויאנים, וכיו"ב.

5.18.1.3. התוכנה נבדקה ע"י בוחני איכות בצורה מעמיקה, באגים הפוגעים באבטחת במידע של המערכת בצורה מהותית תוקנו ולא ידוע לספק על קיום באגים נוספים כאלו.

5.18.1.4. התוכנה נבדקה ע"י חבילת בדיקה מתאימה מפני קוד פוגעני, ווירוסים וכיו"ב, ולא ידוע לספק כי היא כוללת קוד פוגעני שכזה.

5.18.1.5. המערכת לא מבצעת שינויי קוד במערכות נלוות (מערכת הפעלה למשל), אשר פוגעים ברמת אבטחת המידע הכללית של מערכות המחשוב של המזמין.

5.18.1.6. הספק מתחייב כי בגרסאות עתידיות של המערכת לא יתבצעו שינויים מהותיים (להבדיל מבאגים לא צפויים) אשר יפגעו ברמת אבטחת המידע במערכת ללא אישור מפורש מהמזמין.

5.19. ראיות ועדי הספק

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

5.19.2. הספק יתחייב והוא 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.

5.19.3. על הספק להבטיח כי הניטור המתבצע ע"י עונה על דרישות חוק דיני הראיות במלואן.

5.20. אבטחת מידע בניהול משאבי אנוש של הספק

5.20.1. אבטחת מידע בתהליכי גיוס עובדים

5.20.1.1. עובדים המגויסים לארגון יעברו בדיקות רקע, אשר מטרתן לאמת את הנתונים שנמסרו על-ידי המועמד/ת.

5.20.1.2. במשרות רגישות הנוגעות במידע, כפי שיוגדרו על-ידי מנהל אבטחת המידע, יבוצעו בדיקות רקע ואמינות נוספות.

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

5.20.1.4. 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.

5.20.2. אבטחת מידע בעת העסקת עובדים והגברת המודעות שלהם

5.20.2.1. 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.

טל 04-856-4177 פקס 04-856-4363 נייד 050-792-2059
E-Mail: ilanf@rail.co.il

5.20.2.2. יוגדרו נהלים, בקרות ופעולות נוספות המיועדות למנוע את זליגת המידע מעובדים להם יש נגישות למידע של ר"י.

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

5.20.3. אבטחת מידע בסיום העסקת עובדים

5.20.3.1. 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).

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

5.20.3.3. 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'.

טל 04-856-4177 פקס 04-856-4363 נייד 050-792-2059 E-Mail: ilanf@rail.co.il