<u>הנדון: הודעה על כוונה להתקשר עם ספק יחיד לרכישת טובין, עבודות ושירותים</u>

תאריך פרסום ההודעה: 15/09/2025

בהתאם לתקנה 3(18) לתקנות חוק חובת המכרזים (התקשרויות של מוסד להשכלה גבוהה), התש"ע-2010,

בכוונת האוניברסיטה להתקשר עם ספק יחיד: פרולוג'יק בע"מ

מהות ההתקשרות: רכש רישוי, תחזוקה והטמעה של מערכת איילנד (ISLAND) מתוצרת Island Technology Inc

תקופת ההתקשרות: שמונה שנים (שלוש שנים + אופציות להארכה: שלוש שנים+ שנתיים)

אדם הסבור כי קיים ספק ישראלי נוסף המסוגל לבצע את ההתקשרות רשאי לפנות ולהודיע על כך בתוך 10 ימים ממועד פרסום ההודעה ועד ליום 15.10.2025 בשעה 14:00

פניות כאמור יש להעביר בכתב בלבד, באמצעות כתובת הדוא"ל: michraz-haspaka@tau.ac.il

או באמצעות הפקס: 03-6407255

<u>לכל פניה יש לצרף</u>:

1. שם, מען ופרטי התקשרות של הפונה.
2. שם, מען ופרטי התקשרות של הספק המוצע.
3. סטטוס ההתאגדות של הספק המוצע.
4. פירוט בדבר ניסיונו של הספק המוצע ונשוא ההתקשרות.

פנייה אשר תתקבל במען האוניברסיטה לאחר המועד האחרון ו/או פנייה אשר תהיה חסרה איזה מהפרטים הנקובים לעיל, לא תיבחן על ידי ועדת המכרזים.

מצ"ב חוות דעת הגורם המקצועי.

10 בספטמבר 2025

לכבוד

ועדת מכרזים
אוניברסיטת תל אביב

הנדון: **חוות דעת מקצועית במסגרת כוונה להתקשר עם ספק יחיד**

בהתאם לתקנה 3(18) לתקנות חוק חובת המכרזים (התקשרויות של מוסד להשכלה גבוהה) התש"ע-2010, בכוונת האוניברסיטה להתקשר עם ספק יחיד – פרולוג'יק בע"מ.

מהות ההתקשרות: רכש רישוי, תחזוקה והטמעה של מערכת איילנד (ISLAND) מתוצרת Island Technology Inc.

איילנד הינה פלטפורמה מבוססת דפדפן ארגוני מנוהל או כתוסף לדפדפנים קיימים , אשר נותנת מענה להקשחת הדפדפן וגישה מאובטחת לאפליקציות ארגוניות, בקרות על המידע, מניעת דלף מידע ותיעוד על פעולות זדוניות ופעילויות א- נורמאליות , חיבור מאובטח ZTNA ללא צורך בסוכן נוסף מעבר לדפדפן או לתוסף.

שם הספק: פרולוג'יק בע"מ

תקופת ההתקשרות: שמונה שנים (שלוש שנים + אופציות להארכה: שלוש שנים+ שנתיים).

הנימוקים לספק יחיד:

מערכת איילנד נדרשת לאוניברסיטה והנה מערכת יחידה מסוגה מן הטעמים הבאים:

1. גישה מבוססת ZTNA על בסיס דפדפן ארגוני ועל בסיס תוסף לדפדפנים, ללא סוכנים נוספים על תחנת הקצה (Embedded ZTNA) -
גישה מאובטחת מבוססת Zero Trust לאפליקציות פנים ארגוניות משולבת ישירות בדפדפן וכתוסף על דפדפנים קיימים כגון Edge/Chrome, ללא צורך בהתקנת סוכנים או שירותים נוספים . לרבות תמיכה במערכות הפעלה ווינדוס, מק, לינוקס.
   - זמין בשלוש ספקיות הענן המובילות בישראל – היצרן נדרש לתמוך בחיבור של שירות ה ZTNA **בכל שלוש ספקיות הענן המובילות**: מיקרוסופט, AWS וגוגל וזאת עבור שרידות, זמינות וביצועים מיטביים בחיבור של האוניברסיטה.

2. מיתוג ארגוני (Enterprise Branding) בדפדפן + על גבי תוסף לדפדפנים קיימים-
הפתרון יאפשר מיתוג מלא של הממשק לפי הגדרת הארגון, כולל לוגו, פורטל חדשות, עדכונים מותאמים לשולחן העבודה, צבעים והתאמה לעיצוב המערכתי, לרבות ה About Browser והלוגו הפעלה על שולחן העבודה ייחודי לאוניברסיטה.
על הדפדפן להכיל תמיכה בפורטל חדשות ארגוני מתעדכן, לרבות פרסום הודעות מתפרצות, קמפיינים ארגוניים, סקרים והתממשקות למערכות קיימות ב API לטובת פרסום המידע.

3. **תמיכה בהגנת הפרטיות עבור משתמשים** ממיקומים גיאוגרפיים שונים -
המערכת נדרשת לתמוך בשמירת מידע/לוגים של פעולות המשתמש לפי שייכות גאוגרפית באופן אוטומטי וללא ריבוי סביבות ניהול אלא רק עבור שמירת המידע עצמו.
יכולת זו נדרשת עבור חיבור מאובטח של ספקים מהעולם **ועמידה בתקינה בין לאומית**. לדוג': עבור משתמשים אירופאיים המידע יישמר בענן האירופאי, עבור משתמשים אמריקאיים המידע יישמר בענן אמריקאי.

4. תמיכה בחיבור מרוחק ל SMB מובנה בדפדפן עבור גישה מאובטחת מחוץ לרשת האוניברסיטה.
הדפדפן נדרש לתמוך בחיבור מאובטח לתיקיות SMB שיוצגו כפורטל ולא בשורת Address Bar, וללא צורך ברכיב צד ג'. לרבות היכולות, סריקה והגנה על העלאה/הורדה של קבצים, הקלטת ווידאו, תהליך אישור פוזיטיבי, בקרת גישה, DLP ומיסוך מידע.

5. שמירת קבצים במחשבים **לא מנוהלים** על גבי כונן ענני מאובטח-
שמירה בכונן ענני מאובטח ישירות מהדפדפן ונגיש רק מהדפדפן הארגוני לאחר הזדהות, על גבי כונן ענן ייעודי S3 שהיצרן יספק, ללא נוכחות של הקובץ בתחנת הקצה, עם הרשאות גישה, מחיקה אוטומטית, עריכת קבצי אופיס ו -PDF, ושינוע הקובץ בין מערכות ארגוניות.

6. סריקה משולבת OCR/DLP של תוכן וקבצים בתוסף לדפדפנים Chrome/Edge -
מנגנוני סינון, טיהור וסריקה של קבצים ותכנים רגישים באופן אוטומטי לפני הורדה/העלאה או שיתוף . תמיכה ב OCR לטובת מיסוך מזהים רגישים על גבי שכבת הנראות של הדפדפן (DOM) ללא תלות בהורדה/העלאה של קובץ וללא שימוש בפרוקסי.

7. מנהל סיסמאות ארגוני מובנה בדפדפן ובתוסף לדפדפנים Edge/Chrome + יכולת שיתוף סיסמאות מבוקרת (Enterprise Password Manager) -
פתרון מובנה לניהול סיסמאות מאובטח ברמה הארגונית, כולל תיעוד, הצפנה וגישה מבוקרת, לרבות היכולת לשתף בצורה מאובטחת סיסמאות, TOTP מובנה, שינוי סיסמאות חזק ללא חשיפה למשתמש הקצה (Protected Accounts), שמירה של מזהים רגישים API Keys , Secure Notes, בין משתמשי הארגון או קבוצות ארגוניות לפרק זמן קצוב וללא חשיפתם למשתמש הקצה. בממשק ניהול המערכת נדרשת יכולת לבחון בזמן אמת מי שיתף סיסמאות ועבור מי, היסטוריה של החלפת סיסמאות, חוזק הסיסמא, גיל הסיסמא וזאת עבור משתמש מסוים, אפליקציה מסוימת או רק עבור מי ששיתף סיסמאות.

8. פרסום אפליקציות דרך הדפדפן (Publish Client-based Apps) -
תמיכה בפרסום אפליקציות מקומיות (Client-based) למשתמשים באמצעות הדפדפן, כולל אינטגרציה עם Microsoft RDS וכולל גישה ב ZTNA מחוץ לארגון ללא סוכן נוסף מעבר לדפדפן.

9. יכולת תיעוד של ספקים חיצוניים במקרה של אירועי אבטחה וסייבר, התיעוד נדרש להתבצע רק במקרה של אירוע אבטחת מידע/סייבר בצורה אוטומטית, עם אפשרות של - לשונית ספציפית בדפדפן / על כל הדפדפן / כל המתרחש בתחנת הקצה. עבור תיעוד האירועים, נדרשת יכולת של הקלטות ווידאו, הקלטות מקלדת ועכבר ללא תוסף או סוכן נוסף מעבר לדפדפן הארגוני, ורק על בסיס אירוע אבטחה ולא באופן קבוע.

10. ניטור חוויית משתמש בדפדפן ובתוסף לדפדפנים (Digital Experience Monitoring) -
ניטור ביצועים, בדיקה של CPU, Memory, DNS Latency, זמני תגובה וסטטיסטיקות שימוש של ממשק המשתמש דרך הדפדפן ללא סוכנים נוספים על תחנת הקצה לצורכי שיפור חוויית הקצה.

11. תהליך אישור לתוספים (Extension Approval Workflow) -
מנגנון שליטה, בקרה ואישור להתקנת תוספים (Extensions) בדפדפנים, למניעת סיכוני אבטחה.

12. זיהוי פעילות חשודה של מכשירים (Suspicious Device Activity) -
זיהוי וניטור של פעילויות חריגות ממכשירים, כולל התרעות על ניסיונות התחברות חריגים או ניצול לרעה של זיכרון המחשב ושימוש לא לגיטימי בקבצי הדפדפן, במידת הזיהוי תתבצע סגירה אוטומטית של הדפדפן וסגירת החיבוריות של המשתמש עד לאישור חיבור מחדש וזיכוי התרחיש.

13. אוטומציה מותאמת אישית (Custom RPA) -
אפשרות ליצור תהליכי אוטומציה מותאמים אישית על מנת לייעל תהליכי גישה, תגובה ותחזוקה . היכולת נדרשת גם עבור מיסוך מידע, הורדה של פעולות מדפי אתרים, סירוס של פעולות זדוניות ובניית פוליסי מותאם אישית לאקדמיה עם ניסיון מוכח בלקוחות דומים בעולם.

14. ניהול גישה עם הרשאות מורחבות (Privileged Access Management - PAM) -
בקרה על משתמשים עם הרשאות גבוהות בפרוטוקולים סטנדרטים ובחיבור ל Web, RDP, SSH ו SMB .

15. התחזות גלישה בין לאומית לבחירת המשתמש מישראל-
המשתמש יכול לשתף מיקום גאוגרפי שונה ממיקומו באמצעות שימוש בדפדפן בגלישה לאתרים באינטרנט ללא סוכן או תוסף צד ג׳.

16. מחיקת נתוני גלישה ממכשירים לא מנוהלים (Data Wipe & Access Revoke) -
אפשרות למחיקה מרחוק של נתוני גלישה ממכשירים שאינם מנוהלים וביטול גישה בהתאם למדיניות.

על פי הצהרת היצרן (Island Technology, Inc), חברת פרולוג'יק בע"מ הינה המפיץ היחיד בישראל של מערכת איילנד.

אי לכך, בכוונת האוניברסיטה להתקשר עם חברת פרולוג'יק בע"מ לטובת רכש, תחזוקה והטמעה של מערכת ISLAND.

בברכה,

גל יצחק
מנהלת יחידת אבטחת מידע
(CISO)