



סיכום אמצעי האבטחה של HP

כדי להגן על נתוני הלקוח, HP משתמשת בפקדי אבטחת מידע חזקים, לרבות מדיניות, שיטות עבודה, הליכים ומבנים ארגוניים כדי להבטיח שהמידע שלה ושל לקוחותיה יהיה סודי, תקין וזמין (כולל נתונים אישיים כפי שהוגדר בנספח של HP בנוגע ללקוחות ועיבוד נתונים). להלן סקירה כללית של אמצעי האבטחה הטכניים/הארגוניים בחברת HP.

1. מדיניות אבטחה

HP קבעה כללי מדיניות, תקנים ונוהלים גלובליים שמטרתם להגן על הנתונים של HP ושל הלקוחות. פרטי מדיניות האבטחה של HP מסווגים להגנה על שלמות הנתונים והמערכות של HP. עם זאת, בהמשך מופיעים סיכומים של כללי המדיניות המרכזיים שלנו.

2. ארגון אבטחת המידע

תוכנית אבטחת המידע של HP נועדה לנהל ולשמר את הבקורות ואת האסטרטגיות של הארגון לאבטחת מידע. מערכת זו מבטיחה תאימות לבקורות ולמדיניות האבטחה של HP בכל רחבי הארגון וכן ציות לדרישות האבטחה של לקוחותיה. המסגרת מתוכננת בהתאם למסגרות, לחוקים ולתקנות המקובלים בענף לאבטחת סייבר, ועוברת בדיקות שנתיות כדי להסתגל לסביבת האיומים המתפתחת של HP.

3. ניהול סיכונים של אבטחת סייבר

התוכנית של HP לניהול סיכוני אבטחת סייבר נועדה להגן על הסודיות, התקינות והזמינות של נכסי המידע שלה. התוכנית מספקת גישה עקבית לזיהוי והערכה של סיכוני אבטחת סייבר, מיונם לפי סדר עדיפות, טיפול בהם, תיקונם, מעקב אחריהם ודיווח עליהם. HP מגדירה את 'תיאבון הסיכון' שלה כרמה המקובלת לחשיפה לאובדן ואת 'סיבולת הסיכון' כשיעור השונות מ'תיאבון' זה. הערכת הסיכונים מתבצעת באמצעות מתודולוגיה מוגדרת, המאפשרת ל-HP למזער את הסיכונים לאבטחת המידע לרמה מקובלת. התוכנית תואמת לתהליך ניהול הסיכונים הארגוניים של HP.

4. אבטחת HR

המדיניות של HP לאבטחת משאבי אנוש מבטיחה את אבטחת המידע במהלך מחזור חיי העובדים באמצעות קביעת תהליכי גישה למתקנים, מערכות מידע ולנכסים אחרים. זה כולל קבלת אישורים בכתב באמצעות הסכמי סודיות והסכמי אי-חשיפה, וכן ביצוע בדיקות רקע. כל המועמדים להעסקה ב-HP חייבים לעבור בדיקות רקע בהתאם לחוקים, לתקנות ולכללי האתיקה הרלוונטיים.

5. ניהול נכסים

HP קבעה תהליך לזיהוי נכסי מידע טכני, לסיווג נכסים קריטיים לקטגוריות ולניהול הליכי טיפול מתועדים לכל קטגוריית סיווג מידע, כולל קטגוריות שכוללות נתונים אישיים. הליכים אלה מטפלים באחסון, העברה, תקשורת, גישה, רישום ביומנים, שמירה, השמדה, סילוק, ניהול אירועים והתראות על הפרות. התקנים וכללי מדיניות האבטחה של HP כוללים גם את המחיקה המאובטחת של מדיה.

6. אבטחת נתונים

תוכנית אבטחת הנתונים של HP מפרטת את נוהלי האבטחה ואת הבקורות הטכניות שיש ליישם על מנת להגן על הסודיות, על האותנטיות ועל השלמות של הנתונים. בין הגורמים שקובעים כיצד יסווג מידע במדיניות אבטחת הנתונים של HP הם דרישות משפטיות, ערך, חיוניות ורגישות לחשיפה או לשינוי בלתי מורשים. בנוסף לנוהלי הטיפול בנתונים, המדיניות מפרטת הצפנה, מחיקה, איסוף, עיבוד, שמירה וגיבוי של נתונים ומניעת אובדן נתונים.

7. בקרת גישה

HP מיישמת את עקרון ההרשאה המינימלית לבקרת גישה לוגית ומספקת גישה למשתמשים באמצעות מזהי משתמשים ייחודיים וסיסמאות. מדיניות הסיסמאות מגדירה את המורכבות, החוזק והתקינות של הסיסמאות ובקורות של היסטוריית סיסמאות. זכויות הגישה נבדקות מדי פעם ונשללות עם עזיבת עובדים. נוהלים מוסכמים ליצירה ומחיקה של חשבונות משתמשים מיושמים כדי להעניק ולשלול גישה למערכות לקוחות במהלך התקשרויות.

8. קריפטוגרפיה

HP קבעה סדרת תהליכי קריפטוגרפיה חזקה כדי להבטיח את בין היתר, השלמות והזמינות של נכסי מידע. פרוטוקולים שאושרו דורשים הצפנה של נכסים מסוימים, כולל נכסים שכוללים נתונים אישיים. תוכנית הקריפטוגרפיה שלנו כוללת שימוש בטכניקות מתמטיות כדי לאבטח מידע ותקשורת ולהבטיח שרק לגורמים מורשים תהיה גישה לנתונים. אחד הרכיבים הקריטיים בתוכנית אבטחת המידע של HP הוא הגנה על הנתונים מגישה ומשינויים לא מורשים.

9. אבטחה פיזית וסביבתית

מתקני HP מאובטחים באמצעות בקורות גישה פיזיות ואלקטרוניות שונות, כולל אמצעי אבטחה, בקרת גישה אלקטרונית ומצלמות במעגל סגור (CCTV). המתקנים מצוידים גם בתמיכה הנדרשת בתשתית, כולל בקרת טמפרטורה וגיבוי אספקת מתח, שימוש ב-UPS ו/או בגנרטורים לאספקת שירותים חיוניים. כל אנשי הצוות של HP הם רשומים ונדרשים לשאת תגי זיהוי מתאימים.

10. ניהול הפעילות

HP קבעה דרישות מינימום מחמירות לתשתית טכנולוגיה, כולל עמדות עבודה, שרתים וציוד רשת. במכשירים האלה נעשה שימוש בתמונות מוקשות מראש של מערכת ההפעלה, עם דרישות שמשותפות לפי מערכת ההפעלה והבקורות המיושמות. בנוסף, HP פרסה מערכות למניעה/זיהוי של חדירה לרשת (NIDS/NIPS) שמנטרות ומנוהלות מסביב לשעון.

11. אבטחת תקשורת

אבטחת התקשורת מבטיחה הגנה על המידע בתוך הרשתות הארגוניות. זה כולל התקנה וניהול של רכיבי אבטחת רשת (למשל, חומות אש), הפרדה בין רשתית וכן סינון אינטרנט ובקורות לטיפול בדואר אלקטרוני. בנוסף, אבטחת התקשורת כוללת ניטור וניהול של ערוצי תקשורת כדי לזהות ולמנוע גישה בלתי מורשית או הפרות נתונים.

12. אבטחת מערכות

המדיניות של HP מחייבת מתודולוגיית פיתוח מאובטחת של מערכות ותוכנה לאורך מחזור החיים שלהן. מחזור החיים של פיתוח תוכנה כולל התחלה, פיתוח/רכישה, יישום, תפעול וסילוק. כל רכיבי המערכת עוברים הערכה של ההשפעה שלהם על האבטחה הכוללת. HP יישמה בקורות לטרנזקציות בשירותי יישומים, כולל אימות פרטי כניסה של משתמשים, חתימות דיגיטליות, הצפנה, פרוטוקולי תקשורת מאובטחים ואחסון של פרטי טרנזקציות באזור אבטחת רשת מתאים. כמו כן, נערכות גם סריקות קבועות לאיתור נקודות תורפה פנימיות.

13. גורמי צד שלישי וקבלני משנה

HP קבעה תהליכים לבחירת קבלני משנה שתואמים לדרישות אבטחה חוזיים מקיפים. לספקים רלוונטיים שמטפלים בנתוני HP או בנתוני לקוחות, או בעלי גישה לרשת HP, אבטחת הסייבר של HP מבצעת הערכת סיכונים כדי לאמת את תוכנית אבטחת המידע באמצעי הגנה פיזיים, טכניים וניהוליים. הערכה זו נדרשת לפני שהספקים יוכלו לגשת למידע של HP.

14. ניהול אירועים של אבטחת מידע

HP קבעה תהליך מקיף לניהול אירועי סייבר שמתאר את המטרה, ההיקף, התפקידים, תחומי האחריות, המחויבות לניהול, התיאום הארגוני, תהליכי היישום ובדיקת התאימות. התהליך נבדק ומעודכן מדי שנה. צוות התגובה לאירועי סייבר, כולל אנשי אבטחת הסייבר של HP מאומנים בתגובה לאירועים וניהול משברים ומבצע בדיקות מעשיות קבועות של התהליך ושל תקריות ואירועים כלשהם.

15. ניהול המשכיות עסקית

התוכנית הגלובלית של HP להמשכיות עסקית מבטיחה המשכיות מקיפה באמצעות תהליכי תכנון שיתופיים, מתוקננים ומתועדים. מדי פעם החברה מיישמת את תוכניות ההמשכיות העסקית שלה כדי להבטיח יעילות, ובודקת ומעדכנת את כל התוכניות לפחות אחת לשנה. כמו כן, כל העובדים המעורבים בתוכנית ההמשכיות העסקית מקבלים הדרכה מתאימה.

16. תאימות

הגישה של HP לעמידה בדרישות המשפטיות, החוזיות והפנימיות לתוכנית אבטחת מידע יעילה מבוססת על תאימות. בדיקות אבטחת מידע שגרתיות מבטיחות שהפרוטוקולים משולבים בפעילות של כל קבוצה עסקית. כמו כן, תהליך הבדיקה שומר על עדכניות המסמכים כדי לשקף את ההתחייבויות המשפטיות הנוכחיות עם התפתחות הדרישות.

17. ענף כרטיסי התשלום

מסגרת ענף כרטיסי התשלום (PCI) מנחה את הגישה של HP להשגת תאימות לנהלי PCI ומתארת את תחומי האחריות העסקית ואת בקורות האבטחה התואמות ל-PCI DSS. HP מבטיחה עמידה בדרישות ה-PCI באמצעות התקנה ותחזוקה של בקורות אבטחת רשת כמו חומות אש.

18. אבטחת המוצרים של HP

אבטחת המוצרים של HP כוללת נוהלים חשובים לאבטחת מוצרי HP, כמו חתימת קוד, ניהול נקודות תורפה באבטחת המוצר, פרסום עלוני אבטחה ודיווח על בעיות באבטחת מוצרים. אמצעים אלה מבטיחים שמוצרי HP יישארו מאובטחים ומהימנים עבור המשתמשים. לאבטחת המוצרים יש חשיבות עליונה ב-HP מכיוון שהיא עוזרת לשמור על אמון הלקוחות ומגינה מפני אימים פוטנציאליים.

19. אבטחת השירות של HP

אבטחת השירות של HP כוללת נוהלים חשובים לאבטחת השירותים שניתנים ללקוחות HP. המדיניות הזו מטפלת באזורים שונים של אבטחת שירות, כולל אירוח בתשתית HP, אירוח אצל גורמי צד שלישי, אירוח אצל שותפים ואירוח אצל לקוחות. אמצעים אלה מבטיחים ששירותי HP יישארו מאובטחים ומהימנים עבור המשתמשים. הודות ליישום נוהלי אבטחה חזקים, HP מבטיחה את האבטחה והשלמות של המוצרים והשירותים שלה ומטפחת סביבה מאובטחת ואמינה עבור כל המשתמשים.