سياسة البنية التحية

انطلاقاً من أهمية البنية التحتية للأمن السيبراني، تم تحديث البنية التحتية للمدرسة لضمان قدرتها على رصد أي تهديدات ومنع وقوعها، مع الحفاظ في ذات الوقت على قدرة مستخدمي الشبكة على الاتصال بشكل آمن وسلس.

من بين هذه التحديثات نذكر الآتي:

- إضافة خوادم جديدة تتيح اسم مستخدم وكلمة مرور خاصة بكل مستخدم للتأكد من حماية شاملة للمجتمع المدرسي.
- تحديث الجدار الناري الخاص بالشبكة به **Firewall** .
- توفير جدار ناري للموقع الإلكتروني للمدرسة.
- تزويد الموقع الإلكتروني للمدرسة ببرنامج الكوكيز (**cookies**).
- تزويد أجهزة الحواسيب ببرامج حماية ضد الفيروسات.
- إمكانية حجب المواقع الإلكترونية غير المرغوب بها والتي لا تخدم العملية التعليمية.
- تحديث جميع أنظمة تشغيل الحواسيب بالمختبرات ومكاتب الموظفين.
- دعم أنظمة الحماية المعلوماتية لرصد الحوادث الرقمية.
- تحديث نقاط الوصول إلى نظام الإنترنت اللاسلكي (**Access points**) حتى تكون أكثر تطورًا وتغطي جميع مرافق المدرسة.
- استخدام بروتوكول (**IP**) لتشخيص المشكلات التي تحدث في السيرفر.
- منع الدخول للأنظمة الداخلية والخاصة بعد 3 محاولات خاطئة لكلمة المرور.
- تحديث شبكة كاميرات المراقبة **CCTV**، من خلال تركيب عدد من الكاميرات الأمنية الجديدة التي تتيح إمكانية تغطية جميع مرافق المدرسة.

مهام فريق مراقبة البنية التحتية:

- تركيب الخوادم في غرفة خاصة مكيفة يمنع دخولها إلا من الفريق المختص.
- حماية نظام تشغيل الخوادم وتحديثه أسبوعيا.
- تحديث أنظمة تشغيل الحواسيب.
- تركيب برامج حماية الفيروسات ومتابعة مدى فعاليتها ويتم تحديثها تلقائيًا.
- رصد مختلف الفيروسات التي تهدد الأنظمة وإيجاد الحلول الاستباقية.
- التحكم في دخول المستخدمين إلى شبكة الإنترنت ومراقبة مدى سلامة استخدامهم.
- الصيانة الشهرية لأجهزة الحواسيب والتأكد من عملها بفاعلية.

- الاستجابة للحوادث الأمنية والتركيز على مواجهتها بشكل فعال، لمنع المخترقين من تحقيق أهدافهم عبر تفعيل إجراءات استباقية لتجنب حدوثها.
- تفعيل الرقابة على المنصات والتطبيقات التي تستخدمها المدرسة.
- يتم تحديث الجدار الناري بشكل دوري للكشف عن أي هجمات.
- توثيق جميع الحوادث الإلكترونية في ملفات خاصة.
- عمل جدولة لتحديثات البرامج الإلكترونية.