مقرر الأمن السيبراني – التعليم الثانوي
الفصل الدراسي الثالث
بنك الأسئلة – الوحدة الأولى

الدرس الأول - مقدمة في الأمن السيبراني	
1.	**ظهر علم الأمن السيبراني حديثًا قبل حوالي عشرين عام:**
أ	صح
ب	خطأ
2.	**تضمن السرية أن البيانات دقيقة ولم يتم التلاعب بها:**
أ	صح
ب	خطأ
3.	**السرية والسلامة والمصادقة تشكل مثلث أمن المعلومات:**
أ	صح
ب	خطأ
4.	**يتم تطوير جدران الحماية والتشفير لمكافحة الهجمات السيبرانية المتزايدة:**
أ	صح
ب	خطأ
5.	**يؤدي رئيس الأمن السيبراني دورًا وظيفيًا في الأمن السيبراني:**
أ	صح
ب	خطأ
6.	**يتمثل الهدف الرئيسي للهجمات السيبرانية بـ:**
أ	تعزيز البرامج الضارة
ب	التحكم في الشبكة العنكبوتية
ج	الوصول غير المصرح به إلى البيانات
د	جميع ما ذكر
7.	**وظيفة تشفير البيانات في مثلث أمان المعلومات تقوم على:**
أ	حفظ سرية المعلومات
ب	توفير المعلومات بشكل واضح وصحيح
ج	زيادة توفر المعلومات
د	جعل المعلومات أكثر نزاهة
8.	**مصطلح يُشير إلى ضمان إمكانية الوصول إلى المعلومات عند الحاجة:**
أ	السرية
ب	السلامة
ج	التوافر
د	لا شيء مما ذكر

9.	**من المبادئ الأساسية للأمن السيبراني:**
أ	السرية
ب	السلامة
ج	التوافر
د	جميع ما ذكر
10.	**من مجالات التخصص المتعلقة بفئة معمارية الأمن السيبراني والبحث والتطوير التي يصنفها الإطار السعودي:**
أ	تطوير الكوادر
ب	البحث والتطوير في الأمن السيبراني
ج	القوانين وحماية البيانات
د	جميع ما ذكر

الدرس الثاني - مخاطر الأمن السيبراني وثغراته	
1.	**التنصت هو الاعتراض غير المصرح به للاتصالات المختلفة مثل: المكالمات الهاتفية أو الرسائل الفورية:**
أ	صح
ب	خطأ
2.	**منع فقدان البيانات يعتبر من أدوات تحديد مخاطر الأمن السيبراني وتقليلها:**
أ	صح
ب	خطأ
3.	**إدارة التحديثات واحدة من الأنشطة الرئيسة التي تحدد مخاطر الأمن السيبراني:**
أ	صح
ب	خطأ
4.	**حصان طروادة برنامج موثوق يُنفذ إجراءات مفيدة في الخلفية:**
أ	صح
ب	خطأ
5.	**تقوم برمجيات الفدية بتشفير ملفات المستخدم أو الجهاز، وتطالب بالدفع مقابل استعادتها:**
أ	صح
ب	خطأ
6.	**تمثل نقاط ضعف في نظام حاسب أو شبكة، ويُمكن استغلالها من قبل الجهات الخبيثة لإحداث ضرر:**
أ	مخاطر الأمن السيبراني
ب	ثغرات الأمن السيبراني
ج	تهديدات الأمن السيبراني
د	أحصنة طروادة

7.	**من أنواع الجهات المسؤولة عن الهجمات السيبرانية:**
أ	هجمات على مستوى دولي
ب	المنافسون
ج	النشطاء المخترقين
د	جميع ما ذكر
8.	**من أنواع الجهات المسؤولة عن الهجمات السيبرانية، وهم أفراد يستخدمون القرصنة للترويج لقضية سياسية:**
أ	هواة السيكربت
ب	مجموعات الجريمة المنظمة
ج	النشطاء المخترقين
د	المنافسون
9.	**من الأنشطة الرئيسة لتحديد مخاطر الأمن السيبراني:**
أ	مستودع الأصول
ب	التشفير
ج	معالجة المخاطر
د	جميع ما ذكر
10.	**جزء من تعليمات برمجية ترتبط ببرنامج أو بملف آخر، ويتم تنفيذه عند تشغيل هذا البرنامج أو الملف:**
أ	الفيروسات
ب	الديدان
ج	أحصنة طروادة
د	برمجيات الفدية

الدرس الثالث - تهديدات الأمن السيبراني وضوابطه	
1.	**التتبع الإلكتروني لا يعد من تهديدات الأمن السيبراني:**
أ	صح
ب	خطأ
2.	**التفويض يعد وسيلة من وسائل التحكم بالوصول:**
أ	صح
ب	خطأ
3.	**رفع مستوى الصلاحيات لا يعد طريقة من طرائق مهاجمة نظام إدارة الهوية والوصول:**
أ	صح
ب	خطأ

4.	**قد تتطلب أنظمة التحكم في إدارة الهوية والوصول التكامل مع الأنظمة والتطبيقات الحالية:**
أ	صح
ب	خطأ
5.	**تتماثل القرصنة الأخلاقية مع القرصنة الخبيثة من حيث النوايا والسماح:**
أ	صح
ب	خطأ
6.	**من طرق المهاجم في مهاجمة نظام إدارة الهوية والوصول:**
أ	الهندسة الاجتماعية
ب	هجوم القوة المفرطة
ج	هجمات الوسيط
د	جميع ما ذكر
7.	**من الأنشطة الرئيسة التي يؤديها متخصصو الأمن السيبراني:**
أ	ممارسات فريق الأمن الأحمر
ب	الإفصاح والمعالجة
ج	تحديد الأولويات
د	جميع ما ذكر
8.	**من مزايا أنظمة التحكم في إدارة الهوية والوصول:**
أ	سهلة التنفيذ والصيانة
ب	تعتمد بشكل كبير على البيانات الدقيقة
ج	أتمتة العمليات
د	جميع ما ذكر
9.	**وسيلة للتحقق من هوية المستخدم أو الجهاز بصفته شرطًا مسبقًا لمنح الوصول إلى الموارد في النظام:**
أ	عدم الإنكار
ب	التعريف
ج	المصادقة
د	التفويض
10.	**الهدف الرئيسي لنظام IAM هو:**
أ	الحماية من التلف
ب	تشغيل الخوادم بكفاءة أكبر
ج	منع وصول المستخدمين
د	حماية البيانات من التسريب