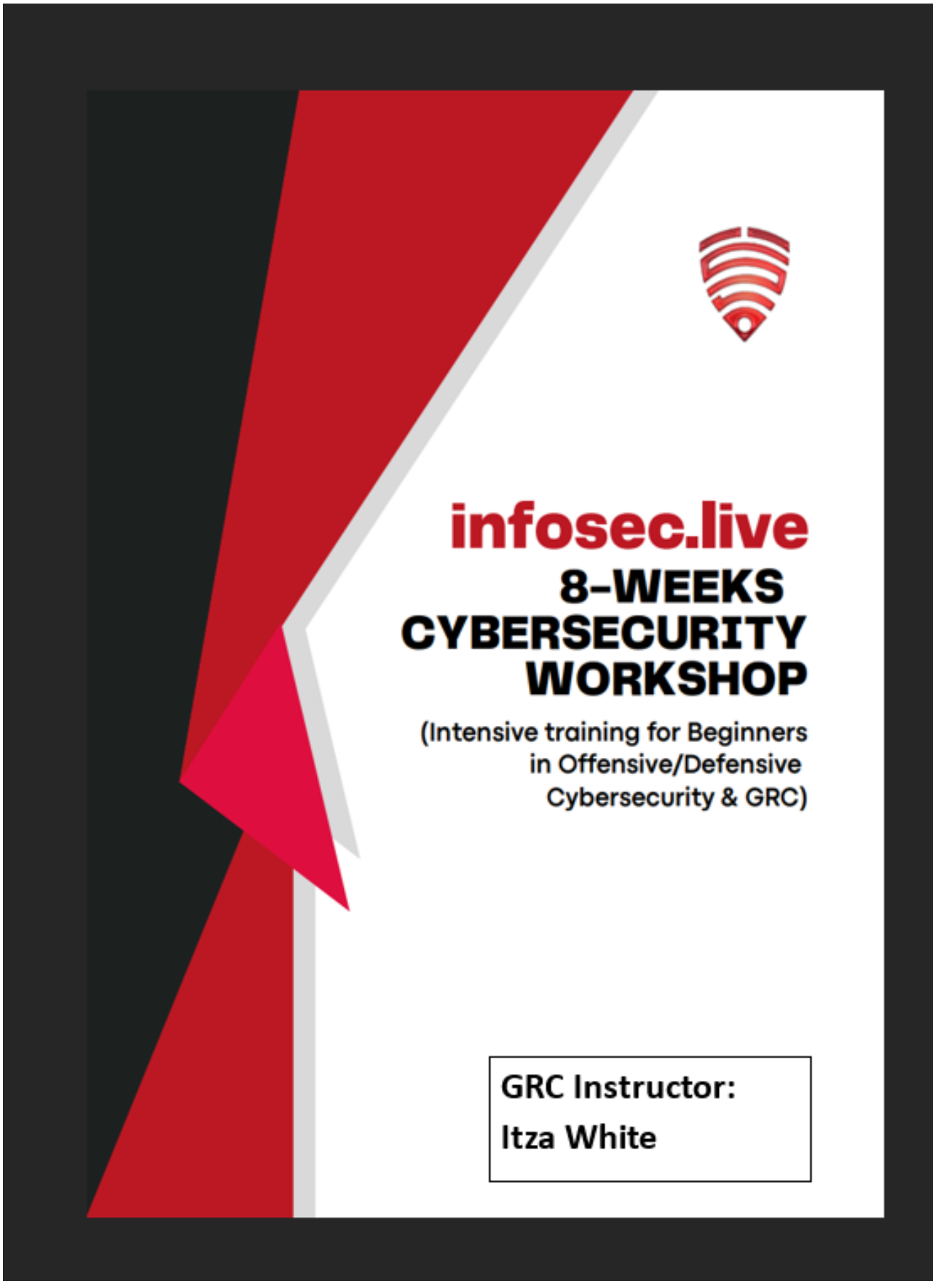


# infosec.live

## 8-WEEKS CYBERSECURITY WORKSHOP

(Intensive training for Beginners in Offensive/Defensive Cybersecurity & GRC)

GRC Instructor:
Itza White

# GRC CAPSTONE

**Security Audit –** A review of an organization's security controls, policies, and procedures against a set of expectations. Audits are independent reviews that evaluate whether an organization is meeting internal and external criteria. Internal criteria include outlined policies, procedures, and best practices. Internal audits are a great way to identify gaps within an organization.

**Establish the scope and goals of the audit.**

Prepare and interview preparation checklist for before, during and after the audit

Establish scope, known risks and goals

Establish the WHY. If the client does not adhere to XXXX. What are the possible risks, fines, loss of revenue, etc.

*Goals: Adhere to NIST CSF*

*Risks: Proper controls are not in place*

After you review the audit scope, goals and known risks consider the following:

- What are the biggest risks to the organization?
- Which controls are essential to implement immediately vs in the future (i.e.) MFA?
- What compliance regulations does this client adhere to ensure the company keeps customer and vendor data safe, avoids fines, etc.?

Conduct a risk assessment of the organization's assets and controls.

Prepare your client, help them prepare for and collect the necessary information and evidence. Provide them with 3-5 questions that will be asked during your meeting

- Review the list of the client's assets
- Review each control name (physical, administrative, technical)
- Review the control types and explanation
- Take note of each control that needs to be implemented
- Note levels of priority (high, medium, and/or low; NA if not applicable)

**Assess compliance.**

The next element is determining whether the organization is adhering to necessary compliance regulations. As a reminder, compliance regulations are laws that organizations must follow to ensure private data remains secure. Such as NIST, ISO27001, GDPR and Payment Card Industry Data Security Standard, or PCI DSS.

Consider where the client conducts business and if they receive payments from customers

Click the boxes to select the compliance regulations and standards that the client needs to adhere to. *

Explain why the client needs to adhere to the selected compliance regulations and standards.

**Communicate results to stakeholders.**

In general, this type of communication summarizes the scope and goals of the audit. Then, it lists existing risks and notes how quickly those risks need to be addressed. Additionally, it identifies compliance regulations the organization needs to adhere to and provides recommendations for improving the organization's security posture. Prepare documentation to present to the client.

Create stake holder memorandum document to communicate:

Scope
Goals
Critical findings
Findings
Summary/ Recommendations

Plan of Action and Milestones/Corrective Action Plan. This will help with budgeting and timeframes. As well as risks that have a high likelihood and high impact should be addressed ASAP

*You can find samples of all of these in the GRC shared drive*

# Create Policies a few examples include:

Here are some of the policies that your company should consider putting in place, please base these on the framework you are working with:

1. Acceptable Use Policy Template
3. Asset Management Policy Template
4. Audit Policy Template
5. Awareness Training and Personnel Security Policy Template
6. Business Continuity and Disaster Recovery Policy Template
7. Change Management Policy Template
8. Encryption Policy Template
9. Identity and Access Management (IAM) Policy Template
10. Incident Response Policy Template
11. Information Classification and Management Policy Template
12. Information Security Policy Template
13. Network Management Policy Template
14. PCI Policy Template
15. Physical Security Policy Template
16. Remote Work Policy Template
17. Risk Management Policy Template
18. System Development and Procurement Policy Template
19. Vendor Management Policy Template
20. Vulnerability Management Policy Template

# Example of AUP (Acceptable Use Policy)

**Acceptable Use**

o Personnel are responsible for adhering to (Company) policies while using our information resources and during company hours. If you have any questions or need clarification, don't hesitate to seek assistance from the Information Security Committee.

o Prompt reporting of harmful events or policy violations involving (Company) assets or information is essential. Please notify your manager or a member of the Incident Handling Team. Examples of reportable events include:

o Technology incidents: Any potentially harmful event that may lead to failure, interruption, or loss of availability to (Company) Information Resources.

o Data incidents: Any potential loss, theft, or compromise of (Company) information.

o Unauthorized access incidents: Any potential unauthorized access to a (Company) Information Resource.

o Facility security incidents: Any damage or potential unauthorized access to a (Company) owned, leased, or managed facility.

o Policy violations: Any potential violations of this or other (Company) policies, standards, or procedures.

o Please refrain from engaging in activities that:

- Harass, threaten, impersonate, or abuse others.
- Degrade the performance of (Company) Information Resources.
- Deprive authorized (Company) personnel access to a (Company) Information Resource.
- Obtain additional resources beyond those allocated.
- Circumvent (Company) computer security measures.

o It is prohibited to download, install, or run security programs or utilities that exploit weaknesses in system security. For instance, running password cracking programs, packet sniffers, port scanners, or any non-approved programs on (Company) Information Resources is strictly prohibited.

o All inventions, intellectual property, and proprietary information developed on (Company) time and/or using (Company) Information Resources are the property of (Company). This includes reports, drawings, blueprints, software codes, computer programs, data, writings, and technical information.

o Encryption should be managed to allow designated (Company) personnel prompt access to all data.

o Please remember that (Company) Information Resources are provided to facilitate company business and should not be used for personal financial gain.

o Cooperation with incident investigations, including federal or state inquiries, is expected from all personnel.

o Respect and compliance with legal protections provided by patents, copyrights, trademarks, and intellectual property rights for any software and/or materials viewed, used, or obtained using (Company) Information Resources are required.

o Intentional access, creation, storage, or transmission of offensive, indecent, or obscene material is strictly prohibited as deemed by (Company).


# PCI-DSS Framework (Level 3)

## TechConnect Mobile

Company Overview:
TechConnect Mobile is a vibrant phone and phone accessory sales company catering to a wide range of customers. We offer the latest smartphones, tablets, wearables, and an extensive selection of accessories. Our dedicated team of professionals provides exceptional customer service and strives to create a seamless shopping experience for every customer.

Organizational Structure:
- Manager/Owner: Jane Goodall
- Assistant Manager: Mark Cuban
- Senior Sales Associates/Key Holders: Emily Ramirez and Michael Jordan
- Full-time Employee: Sarah Connor
- Part-time Employee: Peter Parker

Inventory Management:
TechConnect Mobile utilizes an Excel spreadsheet to track inventory levels, sales, and restocking needs. The spreadsheet includes detailed product information, such as item names, descriptions, quantities, and prices. We conduct inventory counts once a year. Our focus is on sales!

Security Measures:
- Safe Access: Each team member at TechConnect Mobile has an individual code to access the safe, which is used to store cash, valuable merchandise, and sensitive documents. The safe's access code is periodically changed for enhanced security.
- Key Management: All employees are assigned a unique key to the store premises. Keys are carefully monitored, and a key log is maintained to track their usage and ensure accountability.
- We have a camera in the room that has the safe to avoid theft

Sales and Customer Service:
The TechConnect Mobile team is committed to providing excellent customer service, product knowledge, and personalized assistance. Our knowledgeable staff ensures that customers receive expert guidance and support in choosing the most suitable devices and accessories to meet their needs. We update our credit card machines once a year when we conduct a thorough cleaning of the store. We want our customers to feel like family, so we keep their contact information in the back room spreadsheet to ensure if we ever need to reach them we have all of their contact information.

Continuous Learning and Development:
TechConnect Mobile places great emphasis on continuous learning and professional development. Team members regularly participate in training sessions, workshops, and industry conferences to stay updated on the latest advancements in mobile technology, industry trends, and customer service best practices.

Community Engagement:
TechConnect Mobile is dedicated to giving back to the community. We actively participate in local charity events, sponsor local sports teams, and contribute to educational initiatives focused on promoting digital literacy and access to technology. They can reach our website at http://techconnectmobile.com

Network
We use AT&T for our network, all computers are hardwired as well as all POS (Point of sale)
Our customers are family so anyone that need the Wi-Fi can find our password posted on our front desk

Credentials
All employees have their own credentials so we can keep track of sales, their passwords are 10 characters long and change every 6 months
To avoid losing a sale, our senior salespeople write down their codes for the rest of the employees on the whiteboard in the back room. In case an override is ever needed


# ISO 27001

### QuickCover Insurance (6 employees) They will be opening a new office in the EU

Jared Leto - Owner/Manager
Emily Dickenson - Secretary/Administrative Assistant
Alex Dagreat - Intern
Mitchell Pritchett- Insurance Agent
Olivia Munn - Insurance Agent
Sophia Vergara - Insurance Agent

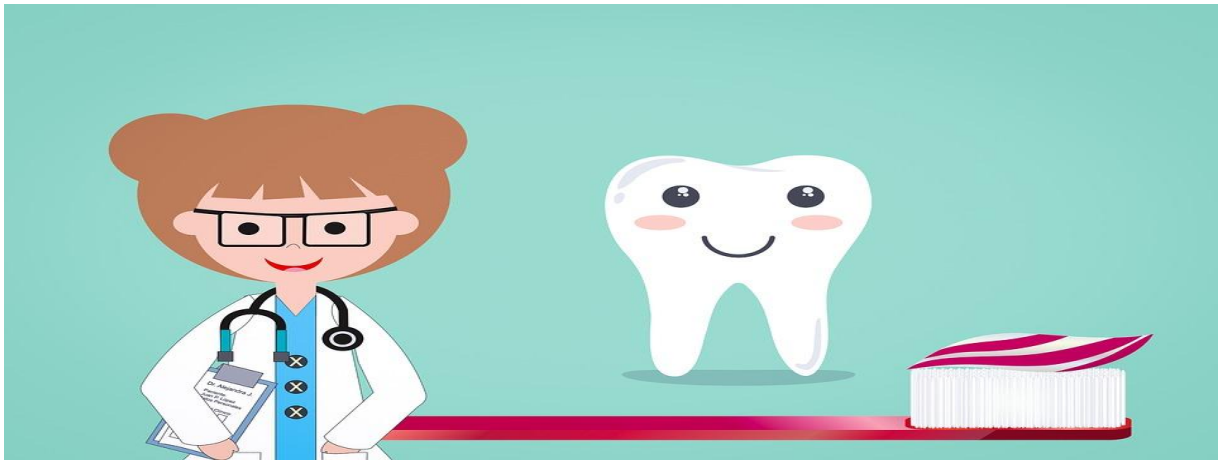
QuickCover Insurance is a small and customer-centric insurance company, specializing in providing a range of insurance solutions to meet the diverse needs of individuals and families. We offer comprehensive coverage options, including auto insurance, motorcycle insurance, home and rental insurance, as well as life insurance. Our priority is to make the insurance process as convenient as possible for our customers, allowing them to email their information to us and receive a quick and accurate quote without any hassle.

Insurance Services Offered:
- Auto Insurance: We offer reliable and affordable auto insurance coverage to protect our customers' vehicles against accidents, theft, and other unforeseen events. Our flexible policies provide the necessary financial protection and peace of mind on the road.
- Motorcycle Insurance: QuickCover Insurance provides specialized insurance coverage for motorcycles, ensuring riders have the necessary protection in case of accidents, damage, or theft. We understand the unique needs of motorcycle enthusiasts and offer tailored policies to meet their requirements.
- Home and Rental Insurance: Our comprehensive home and rental insurance policies safeguard our customers' properties, whether they own a house or rent an apartment. We offer coverage for damages, theft, liability, and more, giving homeowners and renters the confidence to protect their valuable assets.
- Life Insurance: QuickCover Insurance offers life insurance plans that provide financial security and peace of mind for families. Our policies are designed to ensure loved ones are protected financially in the event of the policyholder's untimely passing, offering financial stability during challenging times.

Customer Convenience:
At QuickCover Insurance, we understand the importance of convenience for our customers. To streamline the insurance process, we offer the option for customers to email us their information, allowing us to start the quote process promptly. Our responsive team is dedicated to providing quick turnaround times,

ensuring our customers receive accurate quotes without delay. We aim to make insurance accessible and hassle-free, so our customers can focus on what matters most to them.

Data Security Measures:
QuickCover Insurance understands the importance of keeping customer information secure. We have implemented robust data security measures to protect sensitive customer data from unauthorized access or breaches. Our systems employ encryption protocols and regular data backups to ensure the confidentiality and integrity of client information.



# HIPPA

**BrightSmiles Dental Care (9 employees)**

BrightSmiles Dental Care is a reputable and patient-centered dental practice, committed to providing exceptional oral healthcare services to individuals and families. With a team of highly skilled dental professionals and a warm, welcoming environment, we strive to ensure every patient achieves a bright and healthy smile. Our practice offers a comprehensive range of dental services, including preventive care, cosmetic dentistry, orthodontics, and more.

Organizational Structure:
- Principal Dentist/Owner: Dr. Samantha Williams
- Dental Assistant/Office Manager: Lisa Kudrow
- Dental Hygienists: Sarah Mitchell and Michael Davis
- Front Desk Receptionist: Emily Johnson
- Dental Intern: Alex Trebek
- Cleaning/Custodial: Moe, Larry, Curly

Patient Management:
At Brightsmiles Dental Care, we prioritize efficient and personalized patient management. Our practice utilizes a robust dental practice management software to maintain comprehensive patient records, including medical history, treatment plans, and appointment scheduling. We adhere to strict confidentiality protocols to ensure the privacy and security of our patients' information. We use Dentrix Ascend Software for our EMR/EHR.

Treatment Equipment and Tools:
Brightsmiles Dental Care is equipped with state-of-the-art dental tools and equipment to provide top-quality care to our patients. We regularly maintain and update our dental instruments, including X-ray machines, dental chairs, sterilization equipment, and anesthesia administration tools, to ensure the highest level of safety and effectiveness.

Sterilization and Infection Control:
We maintain rigorous sterilization and infection control protocols to create a safe environment for both our patients and staff. All dental instruments are thoroughly sterilized after each use, and disposable items

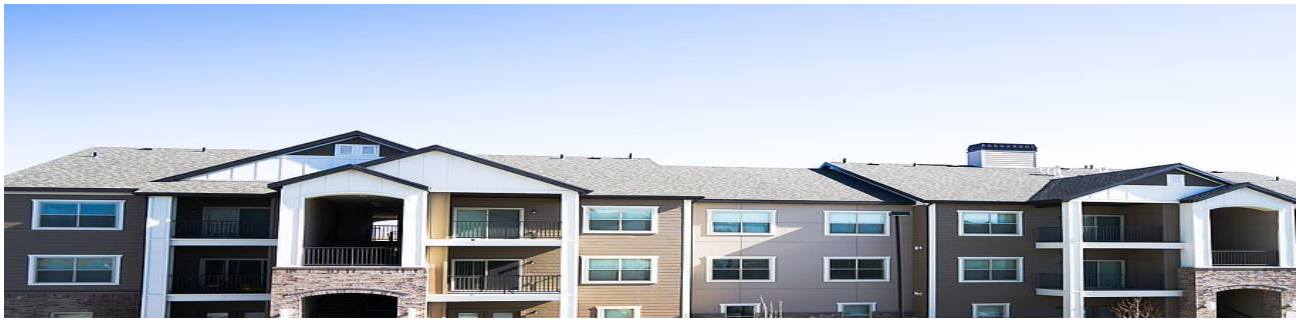
are properly disposed of in accordance with industry guidelines. Our team follows strict infection control measures, including proper hand hygiene, wearing personal protective equipment (PPE), and adhering to standard precautions.

Continuing Education:
At Brightsmiles Dental Care, we value continuous learning and professional development. Our dental team actively participates in continuing education programs, seminars, and conferences to stay abreast of the latest advancements in dental technology, treatment techniques, and patient care. This commitment enables us to provide our patients with the most up-to-date and effective dental solutions.

Community Outreach:
Brightsmiles Dental Care is dedicated to serving the local community. We actively participate in oral health education programs at local schools, community events, and health fairs. We believe in promoting dental awareness and providing access to dental care for all members of the community, regardless of their background or financial circumstances.

Secure Patient Information Management: BrightSmiles Dental Care prioritizes patient privacy and adheres to strict security measures for managing patient information. While we maintain a community laptop for administrative purposes, we ensure that all patient data is securely stored and protected. Access to patient records is restricted to authorized personnel only, we trust everyone in the office and have trained them to only access that community laptop when necessary. We also keep a physical copy of all patient information in the back room in case that computer is being used elsewhere.

Convenient Appointment Scheduling: We understand the importance of convenience for our patients. BrightSmiles Dental Care offers flexible scheduling options to accommodate busy lifestyles. Our team strives to minimize waiting times and provide prompt and efficient dental services, ensuring that our patients receive the care they need without unnecessary delays. Please download our app today! You can find a link for it on our website http://brighsmilesdental.net



# GDPR

## Prime Properties UK: Your Premier Real Estate Partner

Company Overview:
Prime Properties UK is a leading real estate agency based in the UK, specializing in the sale and purchase of properties. With a commitment to excellence and a customer-centric approach, we strive to provide exceptional service and assist clients in finding their ideal properties. Our experienced team of professionals is dedicated to delivering outstanding results and creating long-term relationships based on trust and satisfaction.

Organizational Structure:
- Manager/Owner: Michael Scott
- Assistant Manager: Dwight Schrutte
- Senior Sales Associates/Key Holders: Andy Bernard and Jim Halpert
- Full-time Employee: Ryan Howard
- Part-time Employee: Pam Beasley

Inventory Management:
Prime Properties UK utilizes an efficient system to manage property listings and transactions. Our team utilizes a comprehensive database to keep track of property details, including information such as property types, locations, specifications, and prices. Regular updates and audits are conducted to ensure accuracy and timely availability of property information.

Security Measures:
- Access Control: Each team member at Prime Properties UK is provided with individual access credentials to secure areas within our premises. This ensures restricted access to confidential client documents, financial records, and sensitive information.
- Key Management: All employees are assigned specific keys to ensure secure access to the office and property listings. Key distribution and tracking are closely monitored to maintain a high level of security.

Sales and Customer Service:
At Prime Properties UK, we prioritize exceptional customer service and strive to exceed our clients' expectations. Our dedicated team of professionals is knowledgeable about the local real estate market and provides personalized assistance to clients throughout the buying, selling, or renting process. We are committed to helping our clients make informed decisions and achieve their real estate goals.

Continuous Learning and Development:
Prime Properties UK values ongoing learning and development for our team members. We encourage participation in industry seminars, training programs, and workshops to stay updated on the latest market trends, legal regulations, and innovative real estate practices. This ensures that our team can provide the most up-to-date and valuable advice to our clients.