Company Profile

- *What is the company's full name and what is its legal structure (e.g. corporation, partnership, etc.)*?
  Answer: Smile & Brew Dental Clinic, Solo Proprietorship
- *What is the company's mission and vision?*
  Answer: Mission: To deliver quality dental care with compassion, comfort, and a smile. Vision: To be the trusted clinic that creates healthy smiles in a warm, welcoming space.
- How many employees does the company have?
  Answer: 10
- How is the company's organizational structure set up?
  Answer: 1 chief dentist, 3 associate dentist, 6 dental assistant

Services and Products

- What are the main services or products that the company provides?
  Answer: Provides dental care and oral hygiene services (check-ups, cleaning, fillings, extractions, preventive care, cosmetic dentistry, etc.).
- What problems do these services/products solve for customers?
  Answer: Relieves tooth pain, cavities, and oral diseases. Improves dental health and hygiene. Enhances confidence through better smiles. Prevents future dental problems with proper care and maintenance.
- Who are the company's target customers or clients?
  Answer: Individuals of all ages who need dental care (children, adults, and seniors). Families seeking a trusted dental clinic. Patients needing preventive, restorative, or cosmetic dental treatments. Community members who value both oral health and a welcoming clinic experience.

Operation

- What is the company's daily workflow like?
  Answer: Cleans the receiving/lobby area, so does the treatment area. Prepare all the instruments needed for the treatment. Do inventory and check for the things or materials that lack supply.
- How does the company manage its projects, from start to finish?
  Answer: The owner and employees go into deep planning to identify goals and each has their own tasks to do inside the clinic.
- What key technologies or platforms are central to the company's operations?
  Answer: Facebook Ads, Instagram Ads, and Online Booking **upon hacking and other vulnerabilities, might hire external IT personnel.*

- How does the company handle customer support or client relationships?
  Answer: Personalized Care, Front Desk Service, Follow-ups and Reminders, Social Media Engagement, and Patient Feedback

Data Inventory and Classification

- What types of data does the company handle?
  Answer: Patient's Information, Appointment Records, Billings and Payment
- How sensitive is this data?
  Answer: Every data that the company handles is highly sensitive and not disclosed to everyone.
- How much data is stored and where is it located?
  Answer: The data is stored in a cabinet where the dentists and dental assistants can only access it.

Operational Processes and Data Flow

- How is data collected and processed?
  Answer: As for the patient's record, it is collected by pen and paper where they will fill-out necessary information about themselves so that the dentist is aware of their well-being.
- Who has access to the data?
  Answer: The Dentists and Dental Assistants
- How is data shared with external parties?
  Answer: It is rarely shared unless it is requested.
- What is the data backup and recovery process?
  Answer: The data of the patients are kept as physical records. *There are no backups for this. As for data stored digitally, which are panoramic x-ray records, they are stored in a computer's storage system.*

Existing Security Measures and Governance

- What cybersecurity tools are currently used?
  Answer: There are minimal cybersecurity tools since the data of the patients are paper-based.
- Are there existing security policies and procedures?
  Answer: Patient data is handled with confidentiality. Only authorized employees can have access to their records. It is only shared when the patient requested for it.
- How are employees trained on data security?
  Answer: Employees are trained to handle patient information with confidentiality and care.

- Is there a person or team responsible for IT security?
  Answer: Yes. However, they do not work in the company as they are hired only if there is a problem on one of the machines inside the clinic.

Regulatory and Business Context

- What data protection laws and standards apply to the company?
  Answer: Data Privacy Act of 2012 (RA 10173), DOH Guidelines, Professional Ethics in Dentistry
- What is the potential business impact of a data breach?
  Answer: Loss of Patient Trust, Legal Consequences, Financial Loss, Reputation Damage
- Who are the key stakeholders affected by a security incident?
  Answer: Patients, Destists & Staff, Clinic Owner/Management
- What is the company's disaster recovery plan?
  Answer: Smile & Brew Dental Clinic's disaster recovery plan ensures safety, quick response, clear communication, and secure data restoration. The clinic also implements preventive measures like staff training, system updates, and regular backups to maintain continuous and reliable operations.

Physical Security

- How are your physical locations (clinics, offices, storage areas) secured?
  Answer: Are there security systems, such as alarms, cameras, or access card readers? What is the policy for visitor access? The clinic is secured with locked entrances after operating hours. CCTV is also available to monitor entry points and common areas. As for the visitors, they are only allowed to stay at the waiting area unless they are called upon inside the treatment area.
- How are physical IT assets (if there are any) like servers, network equipment, and workstations protected from theft or damage? Are they kept in locked server rooms or secured cabinets?
  Answer: The desktop that is used for panoramic x-ray is kept inside the x-ray room where only clinic staff are allowed to enter. **Machines used for dental procedures are stored in one room where only staff and patients are allowed to enter. A desktop is stationed on a counter by the clinic's entrance.*
- Do you have measures in place to protect against environmental threats such as fire, water damage, or power outages? (e.g., fire suppression systems, uninterruptible power supplies).
  Answer: A fire extinguisher is available inside the clinic in case of fire emergencies. A rechargeable generator is also available in case of sudden power interruption.

- How do you securely dispose of old hardware, documents, or media that contain sensitive data?
  Answer: Paper records are torn or shredded before disposing to prevent unauthorized access.

Technical Security

- How do you protect your clinic's computer network from online threats? Do you have any tools to block suspicious activity or protect your Wi-Fi?
  Answer: The clinic's Wi-Fi is secured with a password to avoid unauthorized access.
- What do you use to protect your computers and servers from viruses, malware, or other malicious software? How often are these protections updated?
  Answer: Antivirus software is installed on the desktop. Update is applied whenever available.
- How do you control who can access your computer systems and patient records? For example, when a new employee starts or someone leaves, what's the process for giving or removing their access?
  Answer: Only authorized staff have access to the patient data. Access is granted to new employees once trained, and access is revoked when an employee leaves the management. **As their primary form of data is physical, access is revoked through unemployment.*
- How do you make sure your software and computers are up-to-date with the latest security fixes? Do you have a schedule for this?
  Answer: Updates are automatically installed when it is available.
- Do you keep records of what happens on your computer systems, and do you check them for anything unusual?
  Answer: For technical concerns, an external IT technician is consulted to check and repair issues.

Administrative Security

- Do you have any written rules or guidelines for employees on security policies like creating passwords, keeping desks tidy, or handling patient information? How do you let them know about these rules?
  Answer: Clean desk policy, and patient information handling. These rules are communicated during employee onboarding and reinforced through verbal reminders from the management.
- How often do you train your employees on security, and what does that training include? Do you teach them how to spot fake emails or other scams?
  Answer: Staff receive training on confidentiality and proper data handling when hired.

- What would you do if a computer got infected with a virus, a company phone or laptop was lost, or your website/social media page was attacked? Who is in charge of handling that?
  Answer: The clinic owner coordinates response, while the external IT support handles the technical fix.
- How do you assess the security posture of third-party vendors, especially those who handle your data? Do you have security-related clauses in your contracts with them?
  Answer: The clinic occasionally works with external IT providers, insurance companies, or referral specialists. There are no formal security clauses in contracts yet, but vendors are expected to follow professional confidentiality standards.