**Business Case – Enterprise Wireless Network Modernization**

**Executive Summary**

In response to the increasing demand for secure, high-performance wireless connectivity across diverse enterprise environments, this business case outlines a modernization strategy for implementing a robust, scalable, and secure wireless network architecture.

This initiative supports enterprise digital transformation by providing seamless mobility, enforcing identity-based access policies, and supporting modern applications and IoT. Leveraging 802.1X authentication and next-generation Wi-Fi technologies (6/6E/7), this project will improve user experience, streamline IT operations, and align with regulatory and security frameworks.

The target architecture accommodates key enterprise personas including staff, guests, students/customers, and IoT devices while offering flexible deployment options (on-prem, cloud-managed, or hybrid). Vendor neutrality is maintained to preserve optionality and allow organizations to align the solution with existing infrastructure or procurement strategies.

**1. Business Case Summary**

**Objective**  
Implement a secure, scalable, and future-proof enterprise wireless access solution using 802.1X authentication with support for modern identity and access management, visibility, and device segmentation.

**Key Benefits**

* Enhanced security via 802.1X using **EAP-TLS/PEAP**
* Centralized identity and access enforcement (NAC, RADIUS, PKI)
* Dynamic segmentation via **VLANs or user roles**
* Full visibility of **corporate, BYOD, guest, and IoT devices**
* Improved **user experience**, reliability, and throughput with **Wi-Fi 6/6E or Wi-Fi 7**
* Enabler for **Zero Trust Network Access (ZTNA)** and **digital transformation**

**2. Business Case (Initiation)**

**2.1 Focus Areas**

|  |  |
| --- | --- |
| **Focus Area** | **Description** |
| **Business Drivers** | - [University] Campus-wide high-density access - [Retailer] Omnichannel support and real-time inventory - [Bank] Secure access for mobile banking and branch automation |
| **Technology Modernization** | Upgrade from legacy Wi-Fi to Wi-Fi 6/6E/7 for higher throughput, efficiency, and device density |
| **Cost-Benefit Analysis** | - CapEx/OpEx modeling - ROI from reduced outages, faster troubleshooting, and improved productivity |
| **Operational Improvements** | - Zero-touch provisioning - Cloud-based management (optional) - Real-time analytics and monitoring |
| **Compliance and Regulation** | - PCI DSS, ISO 27001, TEQSA, APRA CPS 234 depending on sector |

**3. Business Requirements**

[Purpose through to High-Level Security Requirements]

**4. Options and Considerations (**To Be Expanded in **HLD)**

[options around controller model, identity platforms, segmentation methods]

**5. Next Steps & Recommendations**

**5.1 Immediate Actions**

1. **Stakeholder Engagement**  
   Engage stakeholders from IT, Security, Compliance, Facilities, and Business Units to finalize business and technical requirements.
2. **RF and Site Survey Planning**  
   Schedule preliminary RF assessments and predictive surveys for high-density or high-security locations.
3. **Define Identity Strategy**  
   Align on identity source(s): Hybrid AD, AAD-only, cloud-native IdP, or federated model.
4. **Evaluate Deployment Models**  
   Assess suitability of cloud-managed vs. on-premises wireless controller architecture based on operational model.
5. **Initiate RFP / Vendor Review Process**  
   Develop RFP documentation aligned with the above to evaluate solutions from multiple vendors (Cisco, Aruba, Juniper, Meraki, etc.)

**5.2 Recommendations**

* Adopt **802.1X with EAP-TLS** as the preferred authentication method for corporate and BYOD devices.
* Prioritize **Wi-Fi 6/6E** capable APs to future-proof the investment and support next-gen client devices.
* Implement **Network Access Control (NAC)** to enforce posture and segmentation dynamically.
* Design for **resiliency and redundancy** at the wireless controller, AP, and uplink layers.
* Ensure **guest and IoT segmentation** using separate SSIDs or policy-based roles.
* Integrate wireless telemetry and logs into a **central SIEM or monitoring solution**.
* Embed wireless services in broader **ZTNA and SASE strategies**, especially in banking and retail.