FOR DATA SCIENCE TEAM (DSE Team

□ 1. DSE API endpoint is secure:
□ Uses HTTPS
□ Requires API key authentication
□ Has rate limiting

□ 2. Input validation in AI service:
□ Validate all inputs match expected format
□ Reject obviously wrong data (500 refrigerators)
□ Validate: Monthly spend 0-1,000,000
□ Validate: Equipment hours 0-24

□ 3. Output validation:
□ ROI between 0-100% (or reasonable range)
□ Payback years between 1-20 years
□ Confidence score: 0-1
□ Energy estimate realistic (50-5000 kWh/month)

□ 4. Fallback system ready:
□ Simple calculation if AI fails
□ Mark fallback results as "estimate"
□ Test fallback works when AI service down

□ 5. Response format consistent:
□ Always return JSON
□ Consistent error format
□ Include confidence scores

□ 6. Performance limits:
□ Response within 10 seconds
□ Handle at least 100 requests/minute

□ 7. Model protection:
□ Don't expose model details in errors
□ Monitor for unusual input patterns

Data Security Checklist

□ 1. Training data is clean:
□ No sensitive business data in training set
□ Data is anonymized
□ Remove any personal identifiers

□ 2. Model doesn't memorize sensitive data:
□ Test model doesn't leak training data
□ Validate outputs don't contain private info

□ 3. API key management:
□ Keys stored in environment variables
□ NOT hardcoded in code
□ Rotation plan for keys