# README_QUICK_REFERENCE_CARDS

# SOUTHGATE TERMINAL

## Quick Reference Cards - Team Guide

### How to Use These Cards During the Exercise

---

## OVERVIEW

These Quick Reference Cards are designed to guide each team through a 75-minute cybersecurity incident response exercise. Each card provides phase-by-phase guidance without revealing specific scenario details, allowing teams to respond naturally to events as they unfold.

---

## CARD DISTRIBUTION

Each team receives ONE card specific to their role:

- **EXECUTIVE_QUICK_REFERENCE_CARD.md** - Strategic decisions and stakeholder management
- **MEDIA_QUICK_REFERENCE_CARD.md** - Crisis communications and public relations
- **LEGAL_QUICK_REFERENCE_CARD.md** - Compliance, insurance, and regulatory requirements

- **TECHNICAL_QUICK_REFERENCE_CARD.md** - System investigation and technical response
- **OPERATIONS_QUICK_REFERENCE_CARD.md** - Operational safety and continuity
- **INCIDENT_COORDINATOR_QUICK_REFERENCE_CARD.md** - Multi-team coordination

---

# HOW TO USE YOUR CARD

## 1. Initial Setup (Before Exercise)

- Read through your entire card to understand the flow
- Note the four phases and types of decisions you'll face
- Identify the key documents referenced for your role
- Familiarize yourself with decision frameworks provided

## 2. During the Exercise

- Use phase descriptions to understand where you are in the scenario
- Reference the specific sections as events unfold
- Follow the decision frameworks and checklists
- Use the quick reference sections for rapid decisions

## 3. Key Principles

- Cards guide but don't prescribe - make your own decisions
- Not all events mentioned will happen - respond to what you observe
- Times are approximate - focus on event flow not clock watching
- Coordinate with other teams as situations require

---

# PHASE STRUCTURE

All cards follow the same 4-phase structure:

### Phase 1 (0-15 minutes) - Initial Detection

- Early warning signs appear
- Teams assess and prepare
- Initial coordination begins

### Phase 2 (15-35 minutes) - Escalation

- Multiple issues emerge
- Complexity increases
- External pressure builds

### Phase 3 (35-55 minutes) - Crisis Peak

- Maximum pressure point
- Critical decisions required
- Multiple simultaneous challenges

### Phase 4 (55-75 minutes) - Resolution Push

- Final challenges emerge
- Reporting requirements peak
- Long-term decisions needed

---

## DOCUMENT REFERENCES

Each card references specific documents from the Participant Documents folder:

### Document Types:

- **Immediate Use**: For urgent situations (0-5 minutes)
- **Priority Reference**: For key decisions (5-15 minutes)
- **Detailed Procedures**: For comprehensive guidance
- **Templates**: For documentation and reporting

### Finding Documents:

1. Check your card for document names
2. Use the DOCUMENT_NAVIGATION_GUIDE.md if needed
3. Documents are organised by function:
    - Crisis and Incident Management/
    - Legal and Compliance/
    - Media and Communications/
    - Technical and Operational Procedures/
    - Safety and Emergency Response/

---

## COORDINATION BETWEEN TEAMS

### Information Flow Pattern:

```
 Technical ← → Operations (System status)
     ↓              ↓
Legal ← → Media (Constraints & messaging)
     ↓              ↓
     Executive Team (Decisions)
          ↓
Incident Coordinator (Orchestration)
```

### Key Handoffs:

- **Technical → Operations**: System availability updates
- **Operations → Legal**: Safety and regulatory triggers
- **Legal → Media**: Communication constraints
- **Media → Executive**: External pressure updates
- **All → Incident Coordinator**: Status and needs

---

# DECISION MAKING

### Universal Priority Framework:

1. **Safety** - Always the highest priority
2. **Legal/Regulatory** - Compliance requirements
3. **Operational** - Business continuity
4. **Reputational** - Stakeholder confidence

### When Cards Conflict:

- Safety overrides efficiency
- Legal requirements override preferences
- Team expertise is respected
- Escalate to Executive if needed
- Document decision rationale

---

# COMMON PATTERNS ACROSS ALL CARDS

### Early Warning Signs:

- System anomalies
- Performance degradation
- Unusual behaviour patterns
- External queries

### Escalation Triggers:

- Multiple system involvement
- Safety concerns
- Regulatory requirements
- Media attention

- Resource conflicts

### Critical Decisions:

- Continue vs halt operations
- Manual vs automated procedures
- Transparency vs protection
- Speed vs accuracy

---

## TIPS FOR SUCCESS

### DO:

- Read relevant phase section when emails arrive
- Use decision frameworks provided
- Coordinate with other teams
- Document key decisions
- Reference detailed procedures when time permits

### DON'T:

- Read ahead to future phases
- Share card details with other teams
- Ignore coordination requirements
- Skip documentation
- Make decisions in isolation

---

## QUICK REFERENCE CARD FEATURES

Each card includes:

1. **Phase Guides** - What to expect and when

2. **Decision Frameworks** - How to approach key choices
3. **Document References** - Which procedures to use
4. **Coordination Points** - When to engage other teams
5. **Quick References** - Rapid lookup sections
6. **Templates** - Standard formats for common needs

---

# EXERCISE SUPPORT

### If You Get Stuck:

1. Check your current phase section
2. Review decision frameworks
3. Consult referenced documents
4. Coordinate with other teams
5. Ask Incident Coordinator for guidance

### Remember:

- These cards supplement, don't replace, full procedures
- The scenario will unfold naturally - respond accordingly
- Focus on good decision-making process over "correct" answers
- Document your reasoning for post-exercise review

---

# POST-EXERCISE

After the exercise, cards can be used to: - Review decision points - Identify improvement areas - Update procedures - Train new team members - Prepare for real incidents

---

**Purpose**: Enable effective team response during cyber incident exercise **Method**: Phase-based guidance without scenario details **Outcome**: Natural decision-making with appropriate support

**Version**: 1.0 | **Classification**: All Teams