Title: Howard University Incident Response Playbook

Version 2.0 – September 2025
Prepared by: Cybersecurity Response Planning Team (Updated)
Partners: Microsoft Azure, Cloudforce, Palo Alto (Conceptual UI Reference Only)

🔐 1. Executive Summary

Following the 2021 ransomware attack, Howard University adopted a Microsoft Azure-based cloud infrastructure with deep integration of Sentinel, Defender for Endpoint, Azure Monitor, and Zero Trust architecture. This updated playbook reflects the real infrastructure used by Howard and incorporates lessons learned from the incident, including an emphasis on **annual ransomware simulations**, **annotated workflow diagrams**, and **role-specific views** tailored to different stakeholders.

The Assistant prototype supports an **AI-guided, branching response system** that mimics Palo Alto Cortex XDR for interface usability but aligns with Microsoft tools and best practices.

🛡️ 2. Policy Overview & Objectives

2.1 Purpose

To standardize Howard University's cybersecurity incident response and automate workflows through AI-assisted dashboards.

2.2 Scope

Applies to all faculty, students, staff, IT contractors, and vendors using or interacting with Howard's IT ecosystem.

2.3 Objectives

- Early threat detection using Azure Sentinel alerts
- Fast containment via Defender for Endpoint
- Recovery using secure cloud backups and AD identity restoration
- AI-guided lessons learned tracking & metrics
- Alignment with NIST 800-61, FERPA, HIPAA, and internal compliance

---

📊 3. Threat Classification Framework

Level	Description
Major	Impacts core systems, wide data exposure, or requires law enforcement involvement
Moderate	Affects department-level systems or localized datasets
Minor	No significant impact or data loss; contained internally

Incident evaluation metrics include:

- Service disruption
- Data confidentiality/integrity
- Regulatory exposure
- Recovery complexity

🧩 4. Incident Response Lifecycle

4.1 Preparation

- **Tools in Use:** Azure Sentinel, Microsoft Defender XDR, PIM, Azure Monitor, Log Analytics
- **Training:** Annual user awareness + specialized IT tabletop exercises (including ransomware simulation)
- **Simulation:** Required ransomware drill per academic year

4.2 Identification

- **Detection Sources:** Automated alerts, help desk submissions, behavioral anomalies
- **First Response:** SOC triage using dynamic dashboard w/ AI guidance
- **AI Prompts:** "Outbound traffic anomaly detected. MITRE ref: TA0011. Start guided response?"

4.3 Containment

- Endpoint isolation
- Network segmentation using NSGs and policy automation
- Azure AD conditional access lockdown

4.4 Eradication

- Root cause AI recommendation
- Defender for Endpoint cleansing scripts
- Re-image via cloud deployment templates

4.5 Recovery

- Restore from OneDrive / SharePoint / full Azure BCDR backups
- MFA resets + identity re-verification
- Hardened system baselines reapplied

4.6 Lessons Learned

- AI-generated timeline of skipped/completed tasks
- Post-mortem with annotations
- University-wide debrief and visual reporting to CIO + Trustees

---

👥 5. Role-Specific Views

Analyst View:

- Full technical detail + override capabilities
- MITRE mapping, Defender logs, Sentinel signals
- Playbook ref links, AI guidance

Manager View:

- SLA status, risk heatmaps, completion %
- Summary of impacted units
- Skipped task flags

Client View:

- Plain-language update
- Business/system impact
- Timeline of fix & reassurances

All views pull from the same live incident graph but apply different filters and language framing.

🤹 6. AI Guidance Features

- Step-by-step guidance using adaptive branching logic
- Popups based on Sentinel and Defender telemetry
- Referenced playbook section citations for every action
- "Why This Matters" context blurbs for training

✨ 7. Annotated Diagrams and Interactive Flows

All incident workflows include:

- Annotated step-by-step diagrams
- Branching paths for ransomware vs credential compromise
- Clickable buttons: "Isolate Endpoint", "Review Logs", "Escalate Case"
- Embedded rationale callouts (e.g., "Skipping this step may delay detection by 3+ hours")

🏫 8. Annual Ransomware Simulation Protocol

- Conducted by Cloudforce w/ internal SOC
- Mimics real TTPs based on MITRE ATT&CK updates
- Student involvement via mock communications / fake phishing campaigns
- Results added to lessons-learned section

♻️ 9. Maintenance, Audit & Future Readiness

- Reviewed quarterly
- Updated after each major incident
- Future improvements include:
    - Integration of GPT-based runbook automation
    - Automated tagging of MITRE mappings via Defender
    - Integration of N8N flows for escalations to legal/comms

---

✅ 10. Conclusion

This updated playbook aligns with Howard University's current Azure cloud infrastructure, reflects past lessons learned, integrates AI-driven automation, and supports training, simulations, and compliance. The AI Assistant prototype leverages Microsoft tooling with a Palo

Alto-like interface for usability and guides responders across varying roles in an organized and stress-resilient format.
