BISON Security Program Charter

Office of the Chief Information Security Officer | Enterprise Technology Services

Version 1.0 | Effective Date : September 1, 2026

Document owner	Chief Information Security Officer	**Status**	Draft, pending approval
Program owner	BISON Security Program, Office of the CISO	**Review cycle**	Annual, or on material change
Approval required from	Vice President & Chief Information Officer	**Effective date**	09/01/26
Supersedes	This is the first version effective 9/1/26	**Authority model**	Program authority exercised through the CISO

1. Purpose

This charter establishes the BISON Security Program as Howard University's information security governance, assurance, and coordination function. It defines program responsibilities, the authority delegated to the program through the Chief Information Security Officer, and the obligations of university units that create, operate, procure, or rely on institutional technology and information assets.

Howard University operates an academic enterprise, a hospital and affiliated clinics, a faculty practice plan, federally funded and contracted research, and auxiliary enterprises. These environments create overlapping regulatory, contractual, and operational security obligations. No single control environment satisfies every obligation at the same depth.

The program is therefore chartered to make cyber risk visible, verify control effectiveness, coordinate response, support compliance, and ensure the appropriate executive deliberately accepts unresolved or uncovered risk rather than absorbing it by default.

2. Mission

> *The BISON Security Program enables Howard University's academic, clinical, research, and administrative missions by managing cyber risk, strengthening institutional resilience, supporting regulatory compliance, and promoting secure adoption of techno logy.*

The program is intended to be an enterprise enabling function. Its authority exists to support mission delivery, protect institutional trust, and provide executives with clear accountability for security decisions.

3. Expected Outcomes

The program is accountable for advancing the following outcomes:

- Reduced institutional cyber risk through consistent governance, control assurance, and remediation oversight.
- Improved protection of academic, research, clinical, administrative, and enterprise technology environments.
- Clear executive accountability for accepted or unremediated risk.
- More consistent security review of systems, vendors, integrations, and material technology changes.
- Improved institutional resilience before, during, and after security events.
- Transparent reporting of security posture, open findings, non-coverage, and program performance.

4. Program Responsibilities

The BISON Security Program maintains the governance processes, services, and reporting needed to manage information security risk across the university. These responsibilities apply across the Direct Authority Domain and, through assurance and coordination, across the domains named in Section 5.2.

- Establish and maintain the university information security governance framework.
- Develop and maintain information security policies, standards, baseline configurations, and guidance.
- Assess security risks associated with systems, applications, third-party services, integrations, and material changes.
- Verify control effectiveness and require evidence sufficient to support assurance, audit, and executive reporting.
- Coordinate security incident declaration, severity classification, containment, escalation, recovery support, and post-incident review.
- Support regulatory, contractual, audit, cyber insurance, and institutional risk management requirements.
- Provide security awareness, advisory, architecture, vendor risk, identity, monitoring, and reporting services as defined in the service catalog.
- Maintain the non-coverage register, exception records, open findings, program metrics, and executive reporting materials.
- Identify material gaps in authority, coverage, staffing, service delivery, or resourcing and report them under Section 11.

Program responsibility and CISO authority are intentionally linked, the program accepts accountability for defined services and outcomes, while the CISO exercises delegated authority needed to deliver them.

5. Scope

The program operates in two authority tiers. This distinction is intentional, as the authority delegated through the CISO extends directly within the CIO authority chain. Domains outside that chain receive assurance and coordination unless their accountable executive delegates additional authority.

5.1 Direct Authority Domain

Within this domain, the BISON Security Program may exercise the governance authorities in Section 6 through the CISO. Standards are binding, and remediation direction is mandatory.

- Information systems, applications, and infrastructure operated by or on behalf of Enterprise Technology Services (ETS).
- Enterprise identity, authentication, and access management services.
- University-managed endpoints, networks, and cloud tenancy.
- Third-party services procured through university procurement for institutional use.
- Institutional data in ETS-operated systems, regardless of originating unit.

5.2 Assurance and Coordination Domain

In these domains, the program assesses, advises, reports, and coordinates response. Remediation authority remains with the accountable executive unless otherwise delegated. Each domain must have a named accountable executive.

Domain	Program role
Howard University Hospital and affiliated clinics	Assess, advise, report, and coordinate response.
Faculty Practice Plan	Assess, advise, report, and support joint governance with FPP leadership.
Research enterprise and federally contracted research	Assess, advise, report, and provide control assurance against NIST SP 800-171 and CMMC.
College of Dentistry, the College of Pharmacy, the College of Medicine, and auxiliary enterprises (e.g., Dining Services)	Assess, advise, and report.

6. Security Governance Authority

To fulfill the responsibilities in Section 4, the following authorities are delegated to the BISON Security Program and exercised through the Chief Information Security Officer. This structure makes the authority institutional, durable, and accountable to the approved program rather than personal to any individual officeholder.

- Issue binding information security policies, standards, baseline configurations, and guidance, and require compliance within the Direct Authority Domain.
- Require security assessment before procurement, deployment, integration, data transfer, or material change, and withhold security approval when assessment information is incomplete.
- Direct remediation of identified deficiencies, set risk-based remediation timelines, and require evidence of completion.
- Grant, condition, deny, or revoke exceptions to security policy. Each exception must have an expiration date, named owner, and documented compensating controls when applicable.
- Declare a security incident, classify severity, coordinate response, and direct containment during an active incident, including disconnection or suspension of a system or account when needed to limit harm.
- Suspend or halt deployment, integration, or data transfer that presents unmitigated risk, pending executive review.
- Require access to systems, logs, configurations, contracts, records, and personnel needed for assessment, monitoring, investigation, reporting, or audit support.
- Escalate unresolved findings directly to the CIO and, if unresolved there, to the SVP/Chief Administrative Officer, without intermediate approval.
- Represent the university security position to regulators, auditors, insurers, and counterparties, in coordination with the Office of General Counsel and other appropriate offices.

7. Limits of Authority

These limits ensure the program authority in Section 6 can be granted without ambiguity.

- The program and CISO do not direct clinical practice, academic content, research design, or personnel action.
- Containment actions that would interrupt patient care require concurrence of the clinical house supervisor or designee, except where delay would materially increase patient risk.
- The program and CISO do not accept risks on behalf of the university. Risk acceptance is an executive act under Section 9.
- The CISO does not hold budget authority over units outside Enterprise Technology Services.
- Authority under this charter is delegated by the CIO and may be amended or withdrawn by the approvers in Section 13.

8. Obligations of University Units

To make the program responsibilities and authorities operational, units within the Direct Authority Domain must:

- Submit new systems, applications, third-party services, integrations, data transfers, and material changes for security assessment before commitment or deployment.
- Report suspected security incidents and suspected data exposure to the Office of the CISO without delay and before external notification of any kind.
- Remediate identified deficiencies within the agreed timeline or request a documented exception under Section 6.4.
- Provide access to systems, records, contracts, configurations, logs, and personnel reasonably required for assessment, monitoring, investigation, reporting, or audit support.
- Include security requirements in contracts and statements of work for services that process institutional data.
- Assign unit owners for remediation, exceptions, accepted risks, and evidence requests.

Units within the Assurance and Coordination Domain are expected to meet the same obligations through their accountable executive. If they do not, the resulting gap is reported under Section 11 and recorded under Section 9.

9. Risk Acceptance and Deliberate Non-Coverage

The program does not have resources or authority to cover every domain at equal depth, and it does not represent otherwise. When a risk will not be remediated, or a domain will not be covered, the program documents that decision rather than absorbing it silently.

9.1 Process

- The program documents the risk or uncovered domain, the exposure created, and the remediation or coverage required.
- An executive with authority over the affected domain reviews the risk and, if accepting it, signs the acceptance.
- The acceptance is recorded in the non-coverage register with the accepting executive, date, review date, and related conditions.
- The register is reviewed at least annually and reported under Section 11.

9.2 Standing Rule

> *An unsigned acceptance is not an acceptance. If no executive signs, the risk remains open and is escalated under Section 6.8.*

10. Program Services

This section defines what the program delivers today. The authorities in Section 6 exist to support these services, the outcomes in Section 3, and the responsibilities in Section 4. Services not yet available must be funded or recorded as accepted non-coverage under Section 9.

The catalog reflects current program work, not an aspirational target state. The Office of the CISO maintains the catalog and reports on it under Section 11. Moving a service between tiers does not require charter amendment. Adding or removing a service does.

10.1 Service Tiers

Tier	Definition	Commitment
Established	Delivered on a recurring basis with a consistent owner.	Documented intake and defined service commitment.
Developing	Delivered today, with intake, standards, and coverage still being built.	Best effort. No committed service level.
Emerging	Defined and prioritized but not formally established.	No service commitment. Each is funded or registered under Section 9.

10.2 Service Catalog

> *The catalog currently includes 15 services.*

Service	Tier	Description
Third-Party Security Review	Established	HECVAT and SOC 2 intake, contract cyber-exposure review, vendor reference checks, and assessment readouts to Procurement and counsel.
Security Awareness and Training	Established	Awareness platform administration, phishing simulations, annual awareness programming, and departmental completion reporting.
Governance Representation and Advisory	Established	Standing security participation in technical review, change control, IT governance, AI governance, and audit coordination.
Audit and Assessment Response	Established	Remediation evidence packaging, system security plan artifact validation, unit risk assessment review, and support for entrance and exit conferences.
Security Tooling and License Administration	Established	Ownership, renewal, and configuration of the enterprise security stack, including endpoint detection, privileged credential management, and data governance tooling.

Service	Tier	Description
Identity and Access Support	Developing	Stale account remediation, privileged access enablement, service account provisioning, departure revocation, and conditional access exceptions.
Security Architecture Consultation	Developing	Security design input for network, integration, and endpoint changes, including participation in technical and change review.
Policy, Standards, and Exception Management	Developing	Drafting and review of security policy, standards, baseline configurations, and administration of the formal exception process.
Data Protection and Privacy Support	Developing	Consent and cookie review, electronic discovery support, data loss alert tuning, and transition of key management into the program.
Security Monitoring and Detection	Developing	Alert triage, sign-in and account investigation, log review, and escalation across the detection stack. Dependent on contracted managed security services.
Program Management and Reporting	Developing	Fiscal year objectives, service delivery scorecards, program metrics, and maintenance of this charter and supporting registers.
Incident Response	Emerging	Declaration, severity classification, containment coordination, regulatory clock management, and post-incident review.
Business Continuity and Disaster Recovery	Emerging	Continuity planning, mission-critical application identification, recovery testing, and business impact analysis.
CMMC and Federal Contract Compliance	Emerging	NIST SP 800-171 control implementation, system security plan and plan of action maintenance, and DFARS 7012 obligations for federally contracted research.
Clinical and Faculty Practice Plan Security	Emerging	Security assessment, monitoring, and HIPAA control assurance across the hospital, affiliated clinics, and Faculty Practice Plan.

Emerging services are handled through the non-coverage register under Section 9. Until funded or formally accepted as non-coverage, the program does not represent them as services the university can rely on.

11. Governance, Reporting, and Escalation

11.1 Reporting

Report	Cadence	Audience
Program status and open findings	Monthly	CIO
Risk posture and non-coverage register	Quarterly	CIO; SVP/CAO; Joint Cybersecurity Steering Committee
Incident summary and lessons learned	Per incident, then quarterly in aggregate	CIO; General Counsel; Compliance and Privacy Officer
Annual program report and charter review	Annual	CIO; SVP/CAO; Internal Audit

11.2 Standing Representation

The CISO, or designee, holds a standing seat on the Technical Review Board, Change Control Board, Change Advisory Board, IT Governance Council, and AI governance body. The CISO is also included in procurement review for services that process institutional data.

11.3 Escalation and Dispute

When a unit declines to remediate a finding or disputes a security requirement, the matter escalates in sequence to unit leadership, the CIO, and the SVP/Chief Administrative Officer. At each stage, the finding remains open and recorded. Escalation is a normal program function and is not treated as an exception.

12. Resourcing Assumptions, Constraints, and Program Accountability

This charter is based on the conditions below. A material change to any condition changes what the program can deliver and should trigger review under Section 13.

- Program staffing is five personnel, inclusive of the CISO, with a portion provided through contract staff augmentation subject to renewal.
- Detection and response capability depends on a contracted managed security service. Without that contract, the program cannot commit to continuous monitoring or defined response times.
- Third-party security review currently depends on a single reviewer, creating a key-person dependency the program has identified and is working to remove.
- Authority granted under this charter is a prerequisite to, and independent of, any resourcing request. The program does not treat additional resourcing as a substitute for authority.
- The program is accountable for reporting material gaps in staffing, service delivery, coverage, or execution when those gaps affect the outcomes in Section 3.

13. Review, Amendment, and Approval

13.1 Review and Amendment

The CISO and approvers below review this charter annually and when there is a material change to institutional structure, regulatory obligation, authority, coverage, or program resourcing. Amendments require the same approvals as the original execution. The service catalog, non-coverage registers, and reporting formats referenced in this charter may be updated by the Office of the CISO without amendment, provided the updates remain consistent with this charter.

13.2 Approval

By signing below, each approver establishes the BISON Security Program, ratifies the decisions listed at the front of this document, and approves the authorities delegated in Section 6.