Information Security at Brown

**Computing is an essential part of our day-to-day existence**.
Unfortunately, cyber as well as physical threats abound, putting Brown as well as personal information at risk.

**The Information Security Group (ISG) is charged with mitigating that risk** through the development and maintenance of Brown's information technology security strategy, IT policies and best practices, security training and awareness programs, ongoing risk assessments and compliance tasks. ISG strives to balance **confidentiality** (keeping private matters private), **integrity** (assuring that your information is complete and accurate) and **availability** (having timely and reliable access to your information).

**ISG cannot do this alone. You play a key role in protecting information.** By becoming aware of possible threats and vulnerabilities, you help to protect Brown as well as yourself.

**How to contact us:**

* Call the Brown IT Service Center: 401-863-4357
* David Sherry, Chief Information Security Officer: 401-863-7266
* Patricia Falcon, Policy and Awareness Specialist: 401-863-9259
* Webpage: <http://www.brown.edu/information-technology/information-security>

**Ways to keep informed:**

* Follow us on Twitter:
	+ @CISOatBrownU
	+ @ISGatBrown
* Monthly Brown Bags
* ISG’s *SecureIT* newsletter
* Morning Mail announcements
* Movie nights with panel discussions
* National Cyber Security Awareness Month (October)
* National Data Privacy Month (January/February)
* Staff Development Days
* Request consultations or department visits

**Information Security, Procurement, and Purchasing**

Many contracts and purchases for the university now include specifics and obligations that impact the data and information of the university. There are also laws and regulations that must be followed relative to the ownership, outsourcing, protection, and destruction of Brown information. The Information Security Group wants to highlight some of these areas, and how we can help.

**Where we can provide guidance:**

* Contract reviews:
	+ Cloud-based offerings
	+ Click-through agreements
	+ Hosted services
	+ Third-party service providers
	+ Software purchases
	+ File transfers
	+ Data ownership/custody
	+ Data retrieval
	+ Contractors for disposal of equipment, shredding, scanning and off-site storage
* Audits:
	+ Physical site visits to contracted partners
	+ Review of policies and procedures relative to security and privacy
	+ Reviews of submitted security and privacy documents
* Compliance:
	+ National Association of Information Destruction (NAID)
	+ HIPAA: business associate agreements
	+ Disposition and destruction of IT equipment
	+ Media disposal
* Records management
	+ Destruction and storage of records
	+ Records retention
* Insurance
	+ Breach response
	+ Cybersecurity insurance

**Additional support opportunities by the ISG**:

* Staff meeting participation
* Office best practice security and/or privacy reviews
* PII discovery and remediation
* Hard-drive destruction service
* Guest speakers