BROOKINGS	*Policy Title:* **Internal Privacy Policy**	
	Policy No.	**3**

Responsible Office	**Office of General Counsel**	*Issue Date/ Effective Date*	**10-14-08**
Responsible Officer	**General Counsel**	*Last Revision*	**2-05-09**

1.0 Summary

The Brookings Institution's Internal Privacy Policy establishes Brookings' commitment to ensuring that Confidential Information remains private as well the procedures the Institution has implemented towards the achievement of this goal.

2.0 People Affected

The responsibility to keep Confidential Information private applies to all Brookings employees, to all Brookings affiliates and to all Brookings contractors, regardless of location. Brookings' General Counsel, Chief Information Officer, and Vice President of Communications have additional responsibilities under this policy.

The protections of this policy apply to Brookings employees, former employees, affiliates and former affiliates of Brookings, donors, third parties to whom the Institution owes a contractual or fiduciary duty of confidentiality, and members of the general public who communicate with the Institution via e-mail or the internet, subscribe to the Institution's mailing lists, or attend the Institution's activities or buy goods and services from it.

3.0 Purpose

This *Internal Privacy Policy* has been developed (i) to ensure that every Brookings employee and affiliate understands what confidential and personally identifiable information (PII) is; (ii) to ensure that every Brookings employee and affiliate maintains the security and confidentiality of financial, donor or other sensitive information (collectively, "Confidential Information"), (iii) to ensure that every Brookings employee and affiliate understands what is *not* private at Brookings and (iv) to ensure that every Brookings employee and affiliate understands the circumstances under which Brookings may disclose Confidential Information. Confidential Information is not limited to those items marked "confidential" but also includes information that a reasonable person knows or should know is sensitive, private or proprietary--to Brookings or to a third party to whom Brookings owes a duty of confidentiality. Confidential Information does *not* include scholarly work prepared or collected by an employee as part of his or her work responsibilities, although it may include the underlying data in circumstances where individuals or the Institution has a contractual or fiduciary duty to maintain the confidentiality of such underlying data (e.g., statistical compilations that include PII).

The intent of this Policy is not only to protect the Institution from legal risks associated with the disclosure of Confidential Information, but also to be consistent with the Institution's Code of Ethics, to set forth guidelines to ensure that Brookings employees and affiliates respect the privacy of individuals and treat Confidential Information in a professional manner, and to safeguard the Institution's data integrity, thereby enhancing the Institution's reputation for Quality, Independence and Impact.

PII refers to information that can be used to identify or contact a person uniquely and reliably or can be traced back to a specific individual. PII includes a person's name in combinations with any of the following: relatives' names, postal address, personal e-mail address, home or cellular telephone number, personal characteristics, social security number, date or place of birth, mother's maiden name, driver's license number, bank or credit card information. In some circumstances, a person's name alone may constitute PII.

4.0 Policy Scope

The people whose information is protected by this policy include Brookings employees, former employees, affiliates and former affiliates as well as donors, third parties to whom the Institution owes a contractual or fiduciary duty of confidentiality, members of the general public who communicate with the Institution via e-mail or the internet, subscribe to our mailing lists, attend our activities or buy goods and services from us.

This Policy applies to all Brookings employees, to all Brookings affiliates and to all Brookings contractors, regardless of location. For purposes of this Policy, "affiliate" means any person who has a Brookings title but is not a Brookings employee. This Policy applies to Confidential Information regardless of whether it is kept in an electronic or a paper form or communicated orally.

This document is comprised of this Policy itself, which sets forth the rules and procedures governing privacy at Brookings and a FAQs document, which asks and answers common privacy-related questions. In addition, several other policies interact with this over-arching policy and links to those additional policies are set forth at the end of this document.

5.0 Policy

5.1 General Policy

Brookings will protect Confidential Information in its custody regardless of its source or the form in which it is delivered to or maintained by the Institution. Brookings can and will use Confidential Information, including PII, for its own internal business purposes, provided that those purposes are reasonably related to the purpose for which the information was provided to the Institution. Access to Confidential Information will be limited to those employees with a legitimate organizational purpose to use it.

To the extent Brookings shares Confidential Information with third parties, for example, to deliver employee benefits or to fulfill orders for goods and services or to perform analyses for the Institution (e.g., to study the profile of hits to the website or target marketing of goods or services), Brookings will make commercially reasonable efforts to ensure that such third parties have policies and procedures in place to protect the Confidential Information received from Brookings. Brookings will not disclose, sell or otherwise distribute to any third party any PII without consent, except under the following circumstances:

- Legal requests and investigations—Brookings may disclose any data about an employee, affiliate or third party when, in the judgment of the responsible officers or designated employees, such disclosure is necessary to prevent fraud or to comply with any statute, law, rule, regulation of any governmental authority or any order of any court of competent jurisdiction.
- Third-party service providers and agents—Brookings may, from time to time, outsource some or all of the operations of its business to third-party service providers. In such cases, it will be necessary to disclose Confidential Information (including PII) to those service providers. In some cases, the service providers may collect data directly from employees, affiliates or third parties on behalf of the Institution. Brookings will make commercially reasonable efforts to restrict how such service providers may access, use, store and disclose data. When Brookings employs other companies and individuals to perform functions on its behalf (such as processing compensation, providing employee benefits, and performing legal and other professional services) these agents have access to data needed to perform their functions, but they may not use it for other purposes.
- Protection of the Institution and Others—Brookings may release Confidential Information (including PII) or other information when, in the judgment of Brookings responsible officers or designated employees, release is appropriate to comply with the law; enforce or apply Brookings policies and other agreements; or to protect the rights, property, or safety of Brookings, its employees, or others. This does not include selling, renting, sharing or otherwise disclosing PII from employees, affiliates, guests, or event attendees, for commercial purposes in violation of the commitments set forth in this Policy.
- Debt Collection –From time to time Brookings may use PII to collect debts incurred when people order goods or services and fail to pay for them.
- Security—On occasion Brookings will gather PII from guests invited to events organized by the Institution for the express purpose of sharing it with third parties for security purposes, for example, to permit entry into a government facility or embassy.

Anyone sending *unsolicited* information to Brookings by any means explicitly consents to the storage, destruction, processing, and business use by Brookings of the unsolicited information.

5.2 Employee Privacy

To conduct its business and comply with government regulations (employment, tax, insurance, etc.), Brookings collects various PII and other data from employees and affiliates. The information collected depends on an individual's employment responsibilities, citizenship, location of employment, and other factors. Such data may include one's name, electronic user identifications, passwords, phone numbers, email address, mailing addresses, banking and other financial data, government identification numbers (e.g., Social Security number and/or tax-payer identification number, drivers license, number, etc.), date of birth, gender, race, ethnicity, health and disability data, family-related data (e.g., marital status), personal and health-related data on family members and other necessary information.

Brookings can and will use and share the information it collects about its employees and affiliates to conduct the business of the Institution. This use may include the following general purposes:

- to identify employees or affiliates;
- to communicate with employees and affiliates;
- to comply with human resource requirements;
- to comply with government regulations; and

- to provide employees benefits (compensation, health insurance, etc.).

5.3 Employee Information that Is *Not* Private

Brookings' offices, data storage\processing equipment, telecommunications devices and their contents, services and transmissions are the property of the Institution. This includes any device or service provided by Brookings even if it is partially funded by the individual. Employees, affiliates and contractors should not expect these items to be private. Under certain circumstances, authorized Brookings personnel may enter another person's Brookings office and access paper files kept there. Brookings employees should only access Confidential Information for legitimate organizational purposes.

Brookings can and will monitor computer usage, communications and storage to detect inappropriate content or other materials and to ensure system security and integrity and the safety and security of the workplace. Brookings also uses filters to block inappropriate or malicious content. It is possible that some legitimate content may be blocked by these filters. In addition in the course of normal operations, troubleshooting, or repair authorized Brookings personnel may inadvertently access data. Brookings may provide communications or other services to individuals not affiliated in any way with Brookings, for example, when guests visiting our facilities log in to the Brookings telecommunications network. There is no expectation of privacy in these services.

5.4 Applicant Privacy

Brookings collects PII and other information from people who communicate with the Institution or its staff to inquire about employment. For purposes of this Policy, an "applicant" includes anyone communicating with the Institution about prospective employment or volunteer (internship) opportunities regardless of whether or not the communication was solicited.

Applicants for employment with Brookings voluntarily submit PII and other information to Brookings and the Institution collects additional information on its employment application. The nature of the information Brookings collects will depend on the position an applicant seeks and may include names, phone numbers, email address, mailing addresses and government identification numbers (e.g., Social Security number and/or tax-payer identification number, etc.). Applicants have the option of providing information on gender, race, and ethnicity to assist in ensuring that the Institution complies with various equal employment opportunity rules and to collect data for the Institution's internal diversity initiative.

In addition to information voluntarily submitted and collected as part of the employment application, some applicants may be asked to permit Brookings to conduct a background check. Brookings routinely conducts reference checks on all applicants and submission of an application for employment with the Institution includes express permission to speak with references. Background checks may go beyond speaking with former employers and may include verification of degrees received, credit checks and criminal background checks. Brookings will not conduct background checks on applicants for employment without the applicant's express consent to do so.

Brookings can and will use the information it collects about its employees for the following general purposes:

- To conduct reference checks;
- To conduct background checks;
- To verify eligibility for employment;
- To withhold federal and state taxes if an applicant is hired
- To comply with state new-hire reporting; and
- To facilitate enrollment in company benefits plans.

Brookings protects the information provided by applicants to the same extent it protects employees' information and will only disclose applicant information with the applicant's consent as set forth in this Policy.

5.5 Event Attendance and Website Privacy

There are specific policies that govern Brookings' protection of information collected from visitors to the Institution's websites and of contact lists created and maintained by Communications, the Press, BCEE and various research programs for purposes of outreach. Except as set forth in this Policy, Brookings will not sell PII collected for Brookings outreach or research purposes nor will Brookings use such information for purposes other than the purpose for which the information was collected or purposes reasonably related to the purpose for which it was collected (e.g., to identify "V.I.P.s"). For more information about the Institution's privacy commitments to the public, see the Brookings website Terms and Conditions, Privacy Policy and the Brookings Mailing List Management Policy.

In any mass electronic communications, for example newsletters, Brookings staff must include a link to the Institutions' public (website) privacy policy [http://www.brookings.edu/about/PrivacyPolicy.aspx].

Consistent with Brookings' commitment to public scholarship and open discourse, attendance at Brookings events constitutes a public appearance and participants may be photographed or recorded by Brookings or other media outlets. Likewise, any public commentary, whether at an event or on a public electronic communications medium (on-line forums, chats, blogs, etc.), is not private and Brookings or others may record or quote from participants' contributions. However, to the extent possible, Brookings will continue to treat the PII in its possession as private.

5.6 Customer Privacy

Brookings will collect PII as well as information necessary to facilitate payment for goods and services such as executive education courses, books and journals from its customers. Information collected for such transactions may include the customer's name, address, credit card information email address or phone numbers.

Brookings may use third-party vendors to process its orders. By placing an order, customers consent to Brookings sharing their PII and other information necessary to process orders with such third-party vendors. Brookings may use the information it collects about its customers for the following general purposes:

- To process the order or registration;
- To communicate with customers about the order or registration;
- To survey customers about their satisfaction with the good or service purchased; and
- To advertise similar Brookings goods or services to the customer.

Neither Brookings nor the third-party vendors who assist Brookings in fulfilling orders or registrations will disclose, sell or otherwise distribute to any other party customer information without the customer's prior consent, except as set forth in this Policy.

5.7 Donor Privacy

As a charity, Brookings relies on the generosity of corporate, foundation and individual donors. Unless a donor requests otherwise, Brookings will acknowledge donor contributions in a variety of ways.

Brookings collects Confidential Information from individual donors and from individuals employed or otherwise affiliated with foundations and corporations. Brookings also compiles information about prospective donors from publically available information.

Brookings may use information about donors to solicit additional contributions from existing donors, to identify other prospective donors to the Institution and to communicate with donors about the Institution's activities, including by e-mailing newsletters to donors, inviting donors to public and private events and otherwise communicating with donors about the affairs of the Institution.

Brookings routinely acknowledges donors' contributions in its annual report and other printed materials. Brookings reports the source of its contributions as required or requested in connection with filing various tax returns, updating its credit rating and for other business purposes. If requested to do so by a donor, Brookings will keep donors' identities anonymous to the extent it is legally permitted to do so.

5.8 Contractor and Other Miscellaneous Information Privacy

PII, including social security numbers, may be collected from creditors, suppliers or independent contractors where no tax identification or employer identification number is available. PII so obtained will be subject to the same provisions of the Internal Privacy Policy as those for applicants and employees.

5.9 Retention of Personal Information

Records that include Confidential Information will be maintained in accordance with federal and state laws and internal Brookings policy. When such documents are released for destruction, the records will be destroyed by shredding, burning or, in the case of electronic data, overwriting in a manner which prevents their reconstruction or physical destruction of the media. For further details about record retention and destruction, see Brookings' Document Management Policy and Schedule.

5.10 Access to Sensitive Internal Information

Certain Brookings staff members, by virtue of their positions or functions within the Institution, have the ability to access the information of others. Such access may range from a budgeter's ability to view the budgets of other programs, projects or centers to an ITS staff person's ability access virtually anything stored electronically. It is a violation of this Internal Privacy Policy for a Brookings employee to access information he or she has no legitimate organizational purpose to see. Similarly, Brookings personnel shall not discuss the non-public business affairs of the Institution with others who do not have a legitimate organizational need to know such information.

5.11 Security Measures to Protect Confidential Information

Brookings employs reasonable security measures and technologies, such as individual user password protection, encryption, physical locks, etc. to ensure the protection of Confidential Information. All documents containing Confidential Information shall be stored in locked secured areas and, to the extent practical, clearly marked as "confidential." All computer applications containing Confidential Information shall be maintained on secured, authorized-access data storage and processing equipment only. Only persons who have a legitimate Brookings business reason will have access to Confidential Information. Employees granted such access must take all necessary precautions to ensure the security and integrity of records that include such information when the records are not being used. Such precautions may include, but are not limited to:

- Clearly marking files—whether electronic or paper—in which Confidential Information is stored as "confidential."
- Storing paper documents or files as well as removable electronic media (e.g., CDs or external drives) in a locked room or in a locked file cabinet.
- Not storing Confidential Information on laptops, thumb drives, pdas or home computers or any other medium that would leave Brookings' property;
- Keeping files containing Confidential Information in locked file cabinets except when an employee is working on the file.
- Putting files away, locking or logging off computers and locking both file cabinets and office doors when leaving the office.
- Encrypting sensitive information sent to third parties over public networks (the internet)
- Disposing of paper records containing Confidential Information by shredding, burning or pulverizing them before discarding them.
- Requesting that ITS wipe computer and portable storage devices or physically destroying the medium.

Certain programs or positions that deal with Confidential Information may, in the discretion of the relevant supervisor, be required to maintain a "clean desk" policy. All employees subject to a "clean desk" policy will be so informed by their respective supervisor. Those who are subject to a "clean desk" policy shall tidy their desks and put away all office papers when not in use or at the end of each workday.

5.12 Penalties for Failure to Comply with Policy

Failure to comply with this Policy may result in sanctions, including a formal reprimand in one's personnel file, adverse impact on one's evaluation and any potential raises, termination of one's employment or affiliate status and, for cases of identity theft or other deliberate, unlawful violations of this Policy, civil penalties or criminal prosecution.

6.0 Responsibilities

6.1 All Brookings Employees and Affiliates

Brookings employees and affiliates must make reasonable efforts to keep Confidential Information under their control private and limit the disclosure of Confidential Information to those who have a legitimate organizational purpose for it. Brookings employees and affiliates must follow this policy as well as the related

policies and procedures referenced herein. This includes, to the extent an employee uses or controls Confidential Information, employing the relevant security measures set forth in 1.10 of this Policy.

Brookings employees and affiliates must immediately update the information collected by the Institution when and if it changes so the Institution can maintain accurate data about its employees and so the Institution has current contact information for employees in the event of an emergency. Brookings may maintain prior information about employees; therefore, employees should not expect that all historical data will be removed from files and databases when an employee notifies the Institution of changes.

Under certain circumstances, the Institution may have a public notice duty to inform any affected individual of the disclosure of PII. If anyone becomes aware of a disclosure—deliberate or inadvertent— of PII stored at Brookings, he or she should report the matter to the General Counsel or the Chief Information Officer. The General Counsel (or his or her designee) in consultation with the Chief Information Officer (or his or her designee) will investigate and take, or recommend that others take, appropriate action.

6.2 General Counsel

Brookings General Counsel or his or her designee, in consultation with other relevant Brookings personnel, is responsible for developing or helping to develop employee training and user awareness campaigns, serving as a resource on privacy law and best practices to other Brookings employees and Brookings affiliates, working with relevant personnel to review the privacy and data security policies and procedures of third parties with whom Brookings shares information and working with relevant personnel to respond to disclosures of PII and violations of this Policy.

6.3 Chief Information Officer

Brookings Chief Information Officer or his or her designee, in consultation with other relevant Brookings personnel, is responsible for developing or helping to develop employee training and user awareness campaigns with respect to the appropriate use of internal electronic communications (including e-mail), and electronic communications devices, serving as a resource on data security and best practices to other Brookings employees and Brookings affiliates, working with relevant personnel to review the Institution's privacy and data security policies and procedures of third parties with whom Brookings shares information and working with relevant personnel to respond to disclosures of Confidential Information.

6.4 Vice President of Communications

As the manager of Brookings' websites, the Vice President of Communications or his or her designee, is responsible for developing policies on external electronic communications, such as electronic newsletters and event invitations. The Vice President of Communications or his or her designee also works with the General Counsel and other relevant Brookings personnel to update and enforce relevant Institutional policies and guidelines.

7.0 Implementation and Related Procedures

Under certain circumstances, the Institution may have a public notice duty to inform any affected individual of the disclosure of PII. If anyone becomes aware of a disclosure—deliberate or inadvertent— of PII stored at Brookings, he or she should report the matter to the General Counsel or the Chief Information Officer.

The General Counsel in consultation (or his or her designee) with Chief Information Officer (or his or her designee) will investigate and take, or recommend that others take, appropriate action.

8.0 Supporting Forms/Documents

- Website Privacy Policy
- Mailing List Management Policy
- Conflict of Interest Policy
- Code of Ethics
- Frequently Asked (Privacy) Questions
- Document Management Policy and Schedule (under construction, to come later)

9.0 Approvals

The following Brookings personnel reviewed and approved this Policy:

- General Counsel
- Vice President, Finance and Administration
- Steering Committee (President, Managing Director, Program Vice Presidents)

10.0 Distribution

This Policy should be distributed to all Brookings programs, departments and units.