MONITORING REPORTS
December 2011

2.10 ASSET PROTECTION

Policy: The President shall not allow the Association's tangible, intangible and intellectual assets to be unprotected from undue risk.

Operational definition: The President shall take reasonable measures considered best practice in the management of nonprofit institutions to protect the Association's assets through insurance, policies and procedures, and ongoing monitoring. We believe the risks itemized in the sub-policies provide a comprehensive list of the significant asset risks facing the Association.

Supporting data: See individual policies below.

2.10.1

Policy: [The President shall not] Unnecessarily expose the Association's tangible and intangible assets to loss or damage by theft, embezzlement or other financial fraud, casualty, lack of maintenance, or other cause.

Operational definition: "Tangible assets" refers to real property (land and buildings), personal property (e.g. automobiles, tools, furniture) and financial assets (cash, securities and receivables). "Intangible assets" describes something which a person or corporation can have ownership of and can transfer ownership of to another person or corporation, but has no physical substance, e.g. copyright, trademarks, or patents. In the case of the UUA, our primary intangible assets are copyrights on books, periodicals, and web content and our trademarks. We understand protecting the Association's assets from loss or damage to mean taking the following actions:

To protect tangible assets, the UUA:

- conducts a Facilities Condition Assessment annually,
- develops and monitors security policies and procedures, and
- obtains reasonable levels of insurance.

To protect financial assets, the UUA:

- obtains crime insurance on all employees who handle funds at reasonable levels;
- does background checks on employees who handle funds; and
- documents and enforces policies and procedures regarding the handling of cash, securities and financial transactions.

To protect its intangible assets, the UUA:

- registers and monitors copyrights on all Beacon and Skinner publications

- registers and monitors UUA trademarks

Rationale: Assets are best protected through pro-active polices and procedures that prevent their loss or damage. This includes having a diligent and responsive operations staff, conducting an annual Facilities Condition Assessment, developing procedures that balance safety and security with the culture of openness valued by the UUA, having rigorous financial policies and procedures, and registering and monitoring copyrights and trademarks. When the inevitable losses do occur, assets are further protected through a program of insurance appropriate for the level of risk.

Supporting data:
Physical assets
Facilities Condition Assessment: A Facilities Condition Assessment (FCA) is a process of reviewing all of the building systems (roof, plumbing, HVAC, etc.), estimating when they would have to be replaced based on their useful lives, and calculating the cost of doing so (including a factor for inflation). The UUA conducted such an analysis in each of the last three years and intends to complete the next iteration by January 31, 2012. Thereafter the FCA will be prepared on a three-year cycle. The most recent report shows projected capital maintenance over the next seven years of $4 million. This compares to budgeted capital expenditures for FY 2011 of $306,000. These reports have been reviewed with the Finance Committee and are available for direct inspection.

Ongoing maintenance: The UUA is fortunate to have a Director of Operations with over 20 years of service to the Association and a dedicated staff. He has an intimate knowledge of each of the Association's buildings and reports on their condition twice per month to the Treasurer/CFO. Each year, during the budget process (see policy 2.7.2.B), the Administration prepares a capital budget itemizing investments in facilities necessary to keep the buildings safe and well maintained. This budget uses the FCA as a starting point but varies from it based on resources available and other priorities. The FY12 capital budget, approved by the board at its April 2011 meeting, is available for direct inspection.

Security procedures: The UUA's employee manual specifies security procedures covering:
- Routine and emergency building security
- Emergencies and first aid
- Fire

The employee manual is available for direct inspection.

In December, 2011, the UUA issued emergency procedures guidelines covering the following issues:
- Fire
- Medical emergencies
- Intruders
- Extreme weather
- Bomb threat

The guidelines are available for direct inspection.

Insurance coverage: The UUA maintains a full suite of insurance policies itemized below. Policies and coverage levels are reviewed with the Association's agent and carrier, Church Mutual Insurance Company. In addition, the UUA periodically reviews insurance coverage with a third party insurance consultant. At the end of FY 2011, he advised that the UUA increase its directors' and officers' liability and employment practices coverage limits and move to a different carrier. The UUA carries the following policies:

Policy	**$ Limit**
Multi-Peril	
Property	20,731,090
Business income	1,000,000
General liability	1M each claim/3M aggregate
Directors, officers and trustees and Employment practices liability	5,000,000
Employee benefits liability	1M/3M
Counseling	1M/3M
Workers Comp	500K/500K/500K
Auto	1M/3M
Umbrella	7,000,000
Media	5M each occurance
Fiduciary liability	1,000,000
Crime coverage	1,000,000

Financial assets

Policies and procedures

In their FY07 Management Letter, the UUA's then-current auditors, KPMG, recommended that the UUA develop a complete policy and procedures manual addressing all financial transactions. At that time, the UUA had such a procedures manual, but it was not current and was not complete. The financial services staff has since created a comprehensive policy and procedures manual. KPMG later reviewed the manual and removed this recommendation from the subsequent management letter. The manual is regularly updated to reflect current practices and is available for direct inspection. Part of the audit process is to test selected transactions to insure that they follow written procedures. There were no exceptions noted in the FY 2011 audit report from Mayer, Hoffman McCann.

Background checks

The UUA Human Resources department conducts background checks on all UUA staff (excluding Beacon Press staff, but including Beacon financial staff) as a condition of hire through Oxford Document Management Company. The check includes criminal background (state and county), Social Security Number trace, and credit report review.

Crime insurance

As stated above in 2.10.1, the UUA has obtained $1 million in crime coverage that covers employee dishonesty and ERISA related claims (re: health insurance, retirement plan, and benefits) for all employees who have been subjected to a criminal background check.

Intangible assets

Copyright protection

Both Beacon Press and Skinner House register all published materials with the US Copyright Office and monitor infringements. There is no practical way to systematically detect unauthorized use; one typically learns about infringements, which are very rare in the UUA's experience, through whistleblowers or professional networks. When the UUA is notified of an infringement, legal counsel issues a 'cease and desist' letter to the offending party and follows up with any needed enforcement actions.

Both of the UUA's publishing houses are moving into electronic book publication ("e-books"), which presents many more challenges for copyright protection. The environment for publishing rights is evolving rapidly since each publishing platform (e.g. smart phones, i-Pads, Kindle, Nook, etc.) has its own Digital Rights Management (DSM) rules, which vary significantly one to another. The UUA monitors this rapidly changing landscape by assigning staff to track general and trade news sources and by consulting with legal counsel. The Beacon Press Board of Advisors, which consists of leading professionals in the publishing industry, also provides intelligence about trends and issues in publication rights. Further, Beacon's distributor, Random House, oversees the electronic use of Beacon's copyrighted material including the monitoring of rights, management of permissions, and piracy.

The UUA also carries media insurance coverage of $5 million, which protects the Association should it be accused of violating the copyrights of others in its publishing activities. (See insurance schedule in 2.10.1 above.)

Trademark protection

The UUA has registered its critical trademarks with the US Patent and Trademark Agency and with the Commonwealth of Massachusetts, and the Association employs the services of legal counsel to prepare filings and advise on related legal issues. In the spring of 2010, the UUA, with the advice of counsel, conducted a review of all registered trademarks. It was determined that the list of protected marks was out of date and that the list should be narrowed to those in active use. Additionally, Beacon Press has trademarked the name Beacon Press, their logo and "The King Legacy." Currently, we have registered the following marks:

- Unitarian Universalist Association
- Unitarian Universalist
- The chalice logo we're currently using
- UU World: the magazine of the Unitarian Universalist Association of congregations
- uuworld.org
- Beacon Press

- Beacon Press logo
- The King Legacy

Therefore, I report compliance.

Policy 2.10.2

Policy: [The President shall not] allow the Association to be unprepared to respond to disasters and other crises.

Operational definition: There shall be clear and unambiguous guidelines for crisis response. Crisis, in this instance, refers to a wide variety of disasters: natural, justice-related, and danger to property or persons. Procedures should have role clarity and establish methods of quick communication. Instances of such response by the Association shall be evaluated and the guidelines adapted to capture new strategies.

Rationale: There are numerous causes of and kinds of crisis that can and have affected the Association. It is necessary to have a plan that is flexible, responsive, and based on Unitarian Universalist values. We measure the success of this work with feedback from affected individuals and institutions and by debriefing after each crisis intervention.

Supporting data:
Several years ago, a staff team was formed to create a plan that would address possible crises. A wide variety of institutions and individuals were consulted and the following principles were established as "best practice": that the plan be designed to provide for safety, be simple and clear, be flexible, be responsive, provide appropriate pastoral support, fill a prophetic role where justice issues were involved, be transparent, and to provide quick and effective communication. Additionally, it was agreed that resources needed to be coordinated, that collaboration with appropriate parties would be considered, that clear decision-making authority was needed, that outside resources and expertise be utilized, and that good stewardship be practiced.

Clear procedures for these principles have been established and brought up to date this year. Plans are clear for harm or danger to the Boston buildings, natural and human-made disasters, harm to individuals and reputational harm to leaders, congregations, or the Association. The staff has been educated about those procedures. Guidelines for fundraising opportunities have been developed, considering particularly our relationship with districts and the UUSC. A distinct plan for a major emergency during a General Assembly is brought up to date, reviewed by those responsible, and distributed annually. All of these procedures and guidelines are available for direct inspection.

This year there have been fewer crises than we've experienced in the last several years. We have done fundraising for the following events:

UUA/UU-UNO Uganda Fund	$10,594.97

UUA/UUSC Japan Fund`	$31,851.44
Massachusetts' Tornado Fund	$9,375.31
Total:	$51,821.72

It has been five years since we have experienced problems regarding our response to any crisis. We continue to evaluate our responses for potential changes to policies.

Therefore, I report compliance.

Policy 2.10.3

Policy: [The President shall not] unnecessarily expose the Association, or its Board, volunteers, or staff, to claims of liability.

Operational definition: Claims of liability arise principally from failures to monitor and manage risk. Studies of the Association and its congregations by our insurance carrier, Church Mutual Insurance Company (CMIC), show that most liability claims arise from slip and fall accidents. But the Association also needs to protect itself from "tail risk," that is, events which are extremely rare, but potentially catastrophic such as the sexual abuse of children or sexual harassment. To avoid unnecessarily exposing the UUA to such risks, the UUA has instituted security procedures, staff training, a robust grievance procedure, and a program to monitor the safety of its buildings. In the event that there are claims, the UUA maintains liability insurance to minimize financial exposure.

Rationale: Claims of liability can never be avoided entirely, but robust policies and procedures will minimize claims and provide the strongest defense in the event of a lawsuit. Adequate liability insurance both provides for the expenses of any settlement and legal defense.

Supporting data:
Building safety
Periodically the UUA's insurance carrier conducts safety inspections of the Beacon Hill properties and issues a report with findings and recommendations. The most recent report is available for direct inspection. The UUA and all of its CMIC covered congregations participate in an Association-wide safety program. Annually, UUA staff, including the Treasurer and a representative of Congregational Life, meet with a team from CMIC and review every claim over the past year and significant trends. The team also develops plans to educate congregations about potential sources of liability and methods to address these risks. CMIC prepares a full report and analysis surveying all claims over the last three years. In FY 2011 the security group as a whole experienced 117 claims with losses of $2.1 million representing a loss ratio of 72% (premiums/losses). A ratio of 62% or less earns a premium. The high loss ratio was driven by one large property claim. In the previous four years going back to 2007, loss ratios have ranged from 24% to 54%, an excellent loss history. The report is available for direct inspection.

Security policies
In addition to the most common causes of liability claims, the UUA is cognizant of the relatively low, but potentially catastrophic danger of an armed attack. In light of this, a team of UUA staff has developed enhanced security procedures and protections. As a result, an internet-based video monitoring system was installed for all of our Beacon Hill facilities, procedures were developed to guide staff in responding to an emergency, and a new electronic key card system was installed in January 2011.

Avoiding sexual abuse and harassment
The UUA takes the following steps to minimize the risk of sexual abuse and harassment:

- Written policy for background checks for all UUA staff, including continuous required disclosure for convictions, accusations or charges of physical or sexual abuse;
- Background checks for volunteers with Office of Youth and Young Adults;
- Written policy against harassment;
- Required staff training against sexual abuse, misconduct and harassment (most recently October 27, 2011; October 26, 2011; and October 19, 2010).

Insurance
The UUA maintains the following liability insurance (see policy 2.10.1 above for additional detail):

- general liability
- directors, officers and trustees
- employment practices liability
- employee benefits liability
- counseling
- umbrella liability policy

Therefore, I report compliance.

Policy 2.10.4

Policy: [The President shall not] Unnecessarily expose the Association's intellectual property, information, and files to loss, damage, premature destruction, or improper disclosure.

Operational definition: Protecting intellectual property, information and files involves protecting physical paper files, electronic data files, and archival material. In the course of operating the Association's programs, we collect a large volume of data on staff, volunteers, and congregational members. This includes mailing addresses, email addresses, social security numbers and credit card numbers.

Rationale: Different levels of security are appropriate for different kinds of information. Policies and procedures must address each class of information with the appropriate level of confidentiality and security.

Supporting data:

Intellectual property

See discussion of copyrights and trademarks in Policy 2.10.1 above.

Physical files

Financial and investment files are maintained in the financial services offices and the Treasurer's offices. Non-current files are stored in two locked file rooms in the basement of 25 Beacon Street. Payroll files are kept in locked cabinets in the payroll accountant's office which is locked when she is not present. Archival files of high value are kept in the vault on the 3rd floor of 25 Beacon St. Personnel files are maintained in the locked Human Resources offices in locked cabinets. Confidential files on ministers are maintained by the Ministry and Professional Leadership office. These files have been scanned for electronic filing with the secure DocStar system. It is contemplated that this technology will be applied to other areas of the UUA in the future.

Electronic data files

The UUA's file servers, which house all electronic data files, are kept in a secure room at 25 Beacon Street. Currently the room is locked and the keys are available to authorized personnel only. In January 2011, an electronic key system will be installed which will allow increased control over access. The server room has a specialized fire suppression system and a dedicated cooling system to maintain the servers at ideal operating temperatures. The entire system is backed up daily and tapes removed from the premises and stored at 41 Mount Vernon Street.

Archival material

Essential historical documents, such as board minutes, annual financial reports, general ledgers, etc., are stored in the vault on the 3rd floor of 25 Beacon Street. Only the Treasurer, the assistant to the treasurer, and the Executive Vice President have the combination to the vault. Items such as old congregational files, portraits, A/V material (like reel-to-reel tapes, 35mm film, etc), old glass slides of church buildings are kept in the locked archive storage room in the basement of 25 Beacon. Other archival material has been moved to the Harvard University Library.

Email and mailing addresses

Email addresses are never furnished to 3rd parties. Receipt of an email address from a person implies permission for any business office of the UUA to communicate with that person via email for any purpose. The UUA provides a means for any person with an email address on file at the UUA to indicate their opt-in and opt-out preferences. A database of mail addresses is maintained for the sending of UU World magazine. In addition, the office of Stewardship and Development maintains a database of addresses and other information in Raiser's Edge. This data is on a secure server and is not accessible without authorization.

Confidential information
Confidential data, such as social security numbers and credit card numbers, are subject to evolving regulations and industry guidelines. The UUA has developed policies and systems to insure that our handling of such data will be compliant by the respective deadlines. This involves electronically surveying all of the servers and local storage devices, working with the departments that use such data, and developing policies and protocols to keep the data safe.

Our Data Security and Privacy Policy addresses the collection, use, and safekeeping of data about individuals in the UUA's electronic database. The information is stored in a computer database on the UUA's Boston premises. The computers are in a climate-controlled room that is locked at all times and equipped with a modern fire suppression system. Sensitive data such as employee social security numbers are encrypted within the database. The databases are periodically encrypted and copied to magnetic tape, and the tapes are removed and locked in a different building. There is no direct link between the databases and any public websites.

Online access to the databases requires knowledge of a valid user ID and password. Access to specific types of information, and rights to view or change information, are strictly limited by each authorized person's role as assigned and overseen by both a system administrator and a database administrator.

Information on minors
Personal data about our young people rate an additional level of diligence. Personally identifiable information about individual people under 18 years of age is never made available to anyone outside the UUA. (All UUA staff are subject to criminal background checks prior to employment.) Information about persons younger than 18 has a special flag in the database. That flag prevents the information from being included in any list or being displayed in any other way to an individual or automated process lacking special permissions set within the system to do so.

Therefore, I report compliance.