



**Information Governance and
e-Discovery Readiness Program**

For

Colleges and Universities

July 2010

TABLE OF CONTENTS

I.	Executive Summary	3
II.	What Exactly is Information Governance?	6
III.	So, Why Do I Need This?	8
	A. Cost Avoidance – Mitigating the High Costs of e-Discovery	8
	B. Risk Reduction – Through Appropriate Policies	9
	C. Information Governance Is the New Standard for Excellence	10
IV.	The Information Governance and e-Discovery Readiness Program	11
	Phase 1 – Appropriate Policy	12
	Phase 1 - Benefits.....	12
	Phase 2 – Policy Enforcement	13
	Phase 2 - Benefits.....	14
	Phase 3 – Auditing and Independent Certification	15
	Phase 3 - Benefits.....	15
V.	Conclusion	16

I. Executive Summary

The “computer revolution” has brought about momentous change over the past twenty years in the way society creates, communicates and stores information. Yet, laws and policies have been very slow to adapt to this new paradigm involving immense volumes, high volatility, and great mobility of electronic information.

The reality is that technology is messy. Obsolete tapes sit on shelves, policies are written but not followed, policy enforcement is lax, employees leave, hard drives fail, data gets corrupted, and data growth is exponentially out of control. Moreover, lacking appropriate guidance, individual institutions have been slow to identify and employ comprehensive content management solutions to address the problems associated with the undifferentiated and uncontrolled growth of transmitted and stored data.

Today most information created and received is generated electronically in the form of e-mail messages and their attachments, word processing or spreadsheet documents, web pages, databases and the like.¹ Much of the information is never reduced to paper. Vast amounts of electronic data are created and maintained often without users even knowing that the data has been created, much less saved. Much of this information is vulnerable to compromise and many times lacks adequate security controls or comprehensive data retention policies and oversight through each and every stage of its life cycle.

This information explosion has now made a relatively little understood component of the legal process called **Electronic Discovery (e-Discovery)** both a mandatory and a practical reality.

The question now pressing on colleges and universities across the country is not whether to engage in **e-Discovery**, but rather how to *proactively* integrate **e-Discovery** readiness into their overall **Information Governance (InfoGov)** agenda.

*To assist in this challenge, we are pleased to offer the **iXP Information Governance and e-Discovery Readiness Program**.*

As part of an institution’s overall digital Content Management Program, the goal of this affordable litigation readiness service is to provide colleges and universities with a highly cost effective *internal* **Information Governance and e-Discovery Readiness Program**.

This program is designed to help enhance an institution’s ability to manage its ever growing digital footprint and integrate electronic discovery preparedness and litigation hold requests into routine and reasonable institution processes.

¹ See Lyman, Peter and Hal R. Varian, “How Much Information” 2003, *accessed at:* <http://www.sims.berkeley.edu/research/projects/howmuch-info/summary.html>

The **iXP Information Governance and e-Discovery Readiness Program** is a cost avoidance solution designed to increase an institution's overall **e-Discovery** responsiveness.

This program assesses and closes the three key **Information Governance** gaps, *viewed as critical elements in the eyes of the courts*, for reducing legal liability and massive costs associated with **e-Discovery**:

- **Appropriate Policy**

*iXP will provide professional services guiding institutions through assessment, planning, and implementation of affordable and appropriate **Information Governance** and policy solutions, to include- data retention and litigation hold policies.*

- **Policy Enforcement**

*Targeting, discovering, searching, indexing, identifying, examining, and auditing of the institutions **Electronically Stored Information (ESI)** will be performed for data availability and Payment Card Industry (PCI), Personally Identifiable Information (PII), and data retention policy compliance.*

- **Auditing and Independent Certification**

*The final step of this program will offer institutions regular iXP compliance checks and auditing services. With the ultimate goal of attaining a 100% compliance rating, institutions will be awarded the **iXP System Assurance Integration Framework® (SAIF) Certification** upon successfully achieving a **Silver (80%), Gold (90%), or Platinum (99.9%)** compliance rating in their quest of **Information Governance** perfection.*

Benefits of the iXP Information Governance and e-Discovery Readiness Program include:

Cost Avoidance

- Has your institution EVER been sued? Will it be sued in the future? The e-Discovery process can cost over ***\$18,000 per Gigabyte***.² How big is your institution's digital footprint? How much could it cost you? Reduce your digital holdings and you will reduce e-Discovery costs!
- An effective and properly implemented records management system (including a formal retention and destruction policy) can reduce the universe of records to be searched, and can greatly facilitate the process of identifying repositories of potentially relevant records.
- Fewer records means there is less search time required and fewer documents to review.
- Reduction of cost and risk exposure is direct and immediate.

² "How much can I really save by bringing collection and processing in-house?", eDiscoveryJournal, Barry Murphy, 2010, 5 May 2010 <<http://ediscoveryjournal.com/2010/03/how-much-can-i-really-save-by-bringing-collection-and-processing-in-house/>>

Risk Reduction

- Reduced risk through appropriate policies that are enforceable and focused on your internal culture, that promote work outcomes over employee limits, protect both your institution and your employees, and reduce circumvention and facilitate compliance.
- Having well-organized records reduces the search time required in locating relevant records and the risk of legal sanctions.
- It will allow institutions to react to lawsuits more effectively and help avoid lawsuits altogether.
- Concerns of out of compliance Payment Card Industry (PCI) and Personally Identifiable Information (PII) records are greatly reduced.

InfoGov - A New Standard of Excellence

- Information Governance will turn your universe of data into meaningful information.
- Information Governance transforms information from a vulnerability into an asset by insuring it is consistent, reliable, and available.
- Information Governance insures your knowledge systems will guide users toward quality decisions that meet the vision of your institution's content management.

A detailed explanation of this program may be found on page 11.

II. What Exactly is Information Governance?

When the Amendments to the **Federal Rules of Civil Procedure (FRCP)** took effect in December, 2006, the term **Information Governance** was born.

For every college and university across the country, the security and availability of their information, computer systems, and networks has always been a high priority. For many though, the thought of the institution's **Information Governance** and **e-Discovery** litigation readiness posture may be the last thing on their mind.

At the highest level, **Information Governance** is about managing information better and **Electronic Discovery** is the obligation of parties to a lawsuit to exchange documents that exist only in electronic form (known as **Electronically Stored Information** or **ESI**).

The Economist defines **Information Governance** as the “*strategically created (institution-wide) frameworks that define how information is controlled, accessed and used,*” and the mechanisms that enforce those frameworks.³

The **Association for Information and Image Management (AIIM) International** defines it as “*the establishment of (institution) wide policies and procedures and the execution and enforcement of these to control and manage information as an (institution) resource.*”⁴

Information Governance is a term for a set of activities that have been around for a long time. The term is simple - it places the emphasis of the activity (i.e. governance) on the thing we want to act on (i.e. information). The simplicity of this phrase belies the complexity of a field that borrows ideas and practices from a variety of specialties and packages them together to address a difficult problem in a holistic manner.⁵

For example, **Information Governance** is not synonymous with an institution's operational governance, but it incorporates elements of an institution's operational governance. The same goes for content management, information protection, compliance, and so on. Some of the other fields that are part of an institution's overall **Information Governance** posture include:

- Information Management
- IT Governance
- Privacy
- Knowledge Management
- Records Management
- Document Management
- Disaster Recovery
- Archiving
- Institution-wide Search
- Storage Management
- E-Discovery
- Institution Risk Management
- Institution Administration Continuity
- Governance, Risk and Compliance (GRC)

³ Elizabeth Bennett, “The Future of Enterprise Information Governance,” Economist Intelligence Unit, October 2008.

⁴ AIIM International, “AIIM View On Information Governance,” AIIM Market Intelligence, 2008.

⁵ Barkley T. Blair, “Making the Case for Information Governance,” FCS Information Governance, 2009.

Information Governance is about building a foundation of rules (in the form of policies, procedures, practices, etc.) that guide information management across the entire institution.

Information Governance requires enforcement—in the form of technology and human-focused programs—to be successful.

Information Governance rules themselves do not solve any problems and in fact can create problems if they are not properly enforced. Therefore, it is important that each college and university secures their information, computer systems, and networks, and prepares where it can to appropriately minimize its digital footprint for the scrutiny of legal battle.

The lack of appropriate **Information Governance**, data minimization solutions, and responsive internal **e-Discovery** processing capabilities is now exposing all academic institutions, large and small, to additional and many times unplanned for risk that brings with it the potential of tremendous financial loss.

In order to mitigate the high costs involved in the **e-Discovery** process, colleges and universities must now find the right balance of data retention/destruction policy and enforcement, internal processes for mandatory responsiveness to legal obligations, and integration of new policies and procedures designed to mitigate this growing risk in a way that still aligns with the institution's overarching strategic goals.

Conversely, *reactive* **E-Discovery** processing has left a black eye on many institutions blindsided by the one - two punch of the information growth-information retrieval phenomenon.

While many colleges and universities *have acknowledged the need* to secure information, many more *have yet to embrace* methods for proactively managing their ever growing digital footprint and adequately responding to litigation hold requests as part of their overall content management strategy.

iXP addresses this area of high risk and aims to solve the critical **Information Governance** concerns and **e-Discovery** vulnerabilities plaguing many institutions of higher learning. Through independent assessments, vulnerability identification, gap analysis, and the implementation of new strategies, policies, and crafted solutions, our professional services experts will insure your information management systems will be remain comprehensive, become digitally lean, and remain highly responsive to any internal or external inquiries.

III. So, Why Do I Need This?

A. Cost Avoidance – Mitigating the High Costs of e-Discovery

Let's assume your college or university is involved in litigation involving 20 owners of data, each of whom contributes 10 GBs of data. If an institution turns that data over for processing at an average cost of \$1,000 per GB, the processing alone will cost \$200,000.00. And remember, that's just the cost of processing.

Having a legal team review that data just for responsiveness and privilege will cost more:

- there are typically 7,000 documents per GB
- average review rate is 60 documents per hour
- average blended hourly review rate is \$150 per hour

Therefore, the cost of privilege review for 200 GBs of data will be about \$3.5 million.

Processing and review will total close to \$4 million⁶ . . . but there can also be sanctions!

- **Pension Committee of the University of Montreal Pension Plan v. Banc of America Securities, LLC (S.D.N.Y. Jan. 11, 2010)**
*13 plaintiffs, all of whom were found to be negligent in meeting their e-discovery obligations so as to cause relevant documents to be lost or destroyed. Monetary **sanctions** were imposed on all 13 of these plaintiffs.*
- **A & M Fla. Props. II, LLC, 2010 WL 1418861 (Bankr. S.D.N.Y. Apr. 7, 2010)**
*Court orders monetary **sanctions** for production delay resulting from counsel's failure to become familiar with plaintiff's retention policies and systems*
- **AccessData Corp. v. ALSTE Tech. GMBH, 2010 WL 3184777 (D. Utah Jan. 21, 2010)**
*Court granted **motion to compel** re-production of discovery where initial production was scanned documents converted to PDF format and therefore was not in a "reasonably usable form" pursuant to Rule 34.*
- **Keithley v. Homestore.com, Inc. 2009 WL 816429 (N.D. Cal. Jan. 7, 2009)**
*\$283,000 in fees as a **sanction** and more than \$650,000 of the plaintiffs' legal expenses and costs*
- **Clearvalue Inc. v. Pearl River Polymers Inc., 560 F.3d 1291 (Fed. Cir. 2009)**
***Sanction**, costs and fees of \$121,107.38*
- **Oz Optics v. Kakimoglu, 2009 WL 1017042 (Cal. Ct. App. Apr. 15, 2009)**
***Sanction** \$90,000*

⁶ "How much can I really save by bringing collection and processing in-house?", eDiscoveryJournal, Barry Murphy, 2010, 5 May 2010 <<http://ediscoveryjournal.com/2010/03/how-much-can-i-really-save-by-bringing-collection-and-processing-in-house/>>

B. Risk Reduction – Through Appropriate Policies

Every institution now needs written policies to direct acceptable data retention practices and address expectations of **e-Discovery** litigation hold requests. Traditionally, documented security policies have been viewed mostly as a regulatory requirement. Having a “written policy document” is one of the key controls established within the international standards ISO 27001/27002. Additionally, the Final Security Rule within HIPAA calls for written policy documents as a required control.

Be Aware

- The lack of appropriate data retention and litigation hold policies is a red flag that **Electronically Stored Information (ESI)** security is not a top priority.
- It is also a major factor in the determination of liability in a court of law after an incident.
- An inadequate policy can be as damaging as a lack of policy.
- The effects of legal action due to weak policies can also play heavily against institutions in the court of public opinion as well.
- To maintain their reputation and mitigate litigation costs, institutions must become pro-active and keep and enforce good policies.

A policy provides the “why” and is typically a document that outlines specific requirements or rules that must be met. In the information/network security realm, policies are usually point-specific, covering a single area. For example, an "Acceptable Use" policy would cover the rules and regulations for appropriate use of the computing technologies.

A standard provides the “what” and is typically collections of system-specific or procedural-specific requirements that must be met by everyone. (For example, you might have a standard that describes how to employees classify their files. People must follow this standard exactly if they wish to reduce personal liability and comply with institutional policy.)

A guideline provides the “how” and is typically a collection of system specific or procedural specific "suggestions" for best practice. They are not requirements to be met, but are strongly recommended. Effective security policies make frequent references to standards and guidelines that exist within an (institution).⁷

With over 1500⁸ information security policies actively in use today, iXP’s **e-Discovery Readiness Program** is directed at assessing a college or university’s most critical **Information Governance** policy needs, including data retention and litigation hold policies.

⁷ SANS: Is it a Policy, a Standard, or a Guideline?, <http://www.sans.org/security-resources/policies>

⁸ Information Shield, Inc. *PolicyShield DataSheet.pdf*, <http://www.informationshield.com/information-security-policies.html>, 2008.

C. Information Governance Is the New Standard for Excellence

Colleges, Universities and their employees have a legal duty to preserve, and subject to the rules governing discovery, turn over **Electronically Stored Information (ESI)**.

In short, the law does not offer them a choice. Failure to abide by the law may result in judicially imposed monetary sanctions and adverse findings in the litigation.

Institutions are slowly starting to recognize that **Information Governance** must become an area of focus in order to control both cost and risk. Rule and policy development are prerequisites for making **Information Governance** work.⁹

Most institutions have policies that deal with the proper use of facilities and equipment for institutional purposes. Any policies and procedures addressing information and records management ideally should dovetail with these use policies. Because much of this valuable information is now stored electronically, the need for closer integration of efforts is even greater.

Furthermore, statutes and regulations addressing the privacy rights of individuals (*e.g.*, the *Health Insurance Portability and Accountability Act (HIPAA) of 1996*, *Payment Card Industry (PCI)*, *Gramm-Leach-Bliley Act of 1999*, and security breach legislation in 34 states) have increased the burdens on institutions to ensure that Personally Identifiable Information (PII) data is not improperly disclosed.

Again, since most of this data resides in electronic format, the advantages of relating (existing institutional policies and objectives) to technical and records management solutions become evident.¹⁰

A properly implemented **Information Governance** program will reflect an institution's understanding, commitment, and establish their leadership role in this new **Standard of Excellence**. With it, institutions will be empowered to harness information in a manner that is pro-active, insightful, and reasonable in the eyes of the courts.

⁹ MarketScope for E-Discovery Software Product Vendors, Gartner, 2009

¹⁰ The Sedona Guidelines®: Best Practice Guidelines & Commentary for Managing Information & Records in the Electronic Age, 2007, <http://www.thesedonaconference.org/dltForm?did=Guidelines.pdf>

IV. The Information Governance and e-Discovery Readiness Program

The overarching goal of this program is to provide college and university clients with targeted solutions to mitigate identified gaps and vulnerabilities with regard to their **Information Governance** policies, procedures, enforcement, and litigation response capabilities through a phased approach.

This includes implementing an **Information Governance and e-Discovery Readiness Program** that will help enhance an institution's ability to integrate electronic discovery preparedness and litigation hold requests into reasonable, routine, and easily managed internal institutional processes. A solution designed to move traditionally outsourced **e-Discovery** services inside the institution.

This program will attempt to minimize an institution's ever expanding digital footprint by establishing data retention policies that are customized to the culture of the institution and its operational mandates, to include the determination of local, state, federal or industry regulations applicable to the institution.

By facilitating the streamlining or creation of an internal records management process and **e-Discovery** plan, we will effectively reduce the costs involved in providing **Electronically Stored Information (ESI)** during an active litigation process.

This will be done through assessments and measuring risks surrounding an institution's:

- Current data retention and deletion policies
- Existing records management procedures
- Actual data retention practices
- Existing "digital footprint" size and composition
- Compliance with existing policies and mandates
- Current level of **e-Discovery** readiness

Services and Solution offerings may include:

- The development of appropriate data retention policies
- The streamlining of required records management procedures
- The alignment of stored records against new data retention policies
- The reduction of the institution's overall "digital footprint"
- The reduction of data storage and archive requirements
- The implementation of effective electronic document management solutions
- The development of an **e-Discovery** plan
- The identification of **e-Discovery** team members
- Solutions for pro-active policy compliance auditing and reporting

Program Components

Phase 1 – Appropriate Policy

iXP will provide professional services guiding institutions through assessment, planning, and implementation of affordable and appropriate **Information Governance** and policy solutions, to include a data retention and litigation hold policies.

Phase 1 - Services Offerings Include:

- A Visioning Session
- A Scoping Session
- Systems Identification and Data Mapping
- Systems Information Governance Policy Reviews
- Design and Building of a Gap Analysis and Recommendations Report
- Oversight of Policy Adjustments
- If Required, Oversight of a Policy System Implementation
- Oversight of End User Training Adjustments

Phase 1 - Benefits:

- Institutions will receive customized and appropriate **Information Governance**, data retention, and litigation hold policies that fit the culture of their institution.
- Institutions will receive policies that target identifying and maintaining records, preserving evidence, and increasing responsiveness to electronic discovery requests.
- Institutions will receive policies that balance the level of academic control with a level of employee productivity.
- Institutions will receive the understanding that not all policy controls are possible or required and not all records must or should be retained indefinitely.
- Institutions will receive a greater understanding of how management has the ultimate level of control over policy development, implementation, enforcement, and liability to include litigation readiness.
- Institutions will gain clarity, insight, and vision on the value of **Information Governance** toward cost avoidance and increased academic profitability.

Phase 2 – Policy Enforcement

As part of the **e-Discovery Readiness** portion of the Program, the targeting, discovering, searching, indexing, identifying, examining, and auditing of the institutions **Electronically Stored Information (ESI)** will be performed for data availability and PCI, PII, and data retention policy compliance.

An **e-Discovery** hardware appliance will be installed on the institution's network to perform this function. Using appliance software, technicians will search all public and private file locations including all laptops, desktops, servers, archives, and backups.

The **e-Discovery** appliance will be used to generate reports at the stages of network discovery, indexing, and query results. An appropriate schedule for network discovery, indexing of documents, and queries will be defined with the client institution. Armed with these reports internal institution IT staff and legal counsel may embark on a data minimization plan and any needed corrective actions to mitigate out of compliance findings.

With the institution's digital footprint effectively reduced through newly established data retention policies and records management house cleaning, iXP program experts will offer project management services to guide the institution's internal preparation for litigation hold requests for **ESI** through the development of a formal **e-Discovery Readiness Plan**. Any institution that reasonably anticipates litigation as an incident of day to day operations will ultimately benefit from pro-actively implementing an **e-Discovery Readiness Plan**.

The plan should, among other things, include references to the institution's data retention policies and records management procedures, procedures and forms for implementing a litigation hold, designate a person responsible for responding to discovery requests, prescribe procedures for conducting searches for relevant records (including identifying any tools to be used in searching for records), and identify any internal IT personnel or external litigation support consultants the institution may wish to contact.¹¹

Phase 2 - Services Offerings Include:

- Indexing Appliance Tool Selection
- Install Tool and Index Environment
- Review and Analyze Data Map Findings with Client
- Identify Out of Compliance Data
- Develop a Compliance Clean Up Plan
- Establish a "Steady State" Compliance Clean Up Schedule
- Development of an e-Discovery Readiness Plan
- Develop an Institution wide Data Reduction Plan

¹¹ Ontario e-Discovery Implementation Committee, 10 Guiding Principles to Minimize e-Discovery Costs, 2009, http://www.oba.org/en/publicaffairs_en/E-discovery/model_precedents.aspx

Phase 2 - Benefits:

- Institutions will reduce their requirements for data storage and receive assurance their new digital footprint not only fits the culture of their institution but adheres to all governing mandates and policies for records retention.
- Institutions will have received professional consultation services to assist in the development of an internal **e-Discovery Readiness Plan**.
- Institutions will have matured to the level of establishing **e-Discovery** readiness as a regular institutional process.
- Institutions will have built an **e-Discovery** readiness team to include a designated legal counsel, IT, records, finance, and institutional management, whose due process is fully defined by written policy and, where needed, the best **e-Discovery** vendors and experts in the field.

PROGRAM ADVISORY NOTE - PHASES 1 & 2:

Due to the extremely critical factors surrounding assumed liabilities, legal mandates, and applicable regulatory requirements with regard to the development and implementation of institutional policies, iXP consultants shall serve solely as professional services domain experts for policy solution facilitation; identification of and recommendations for appropriate e-Discovery response team member participants; and the facilitation of e-Discovery Readiness Plan development.

Actual policy creation, final policy content, e-Discovery Readiness Plan creation, and final plan content shall fall exclusively within the institution's domain and control. All policies and plans shall receive guidance, validation, and final approval from the institution's legal counsel to ensure they are complete, reasonable, and appropriate prior to their release and implementation.

Phase 3 – Auditing and Independent Certification

The final step of this program will offer institutions regular iXP compliance checks and auditing services. With the ultimate goal of attaining a 100% compliance rating, institutions will be awarded the **iXP System Assurance Integration Framework® (SAIF) Certification** upon successfully achieving a **Silver** (80%), **Gold** (90%), or **Platinum** (99.9%) compliance rating in their quest of **Information Governance** perfection.

Monitoring compliance with data retention and litigation hold policies is not yet required by law, but is a matter of sound practice and may provide for safe harbor from liability. An institution can enhance its prospects for a successful retention program—and reduce its risk of exposure—if it conducts *independent* periodic reviews and takes meaningful steps to improve compliance with the program.

The review of end user storage habits during the information housekeeping process, or the process of a litigation collection, may also uncover electronic “pack rats” or the improper use of the institution’s information assets. While not part of a formal review process, this new channel for feedback to those responsible for monitoring and updating the (institution’s) records management program can be beneficial.¹²

Phase 3 - Services Include:

- Auditing Appliance Tool Selection
- Determine Scope of Audit
- Install Tool and Index Environment
- Review and Analyze Data Map Findings with Client
- Identify Out of Compliance Data
- Monitor Client Remediation for Out of Compliance Data
- Re-Indexing for Compliance Verification
- iXP’s SAIF® Tiered Compliance Certification

Phase 3 - Benefits:

- Institutions develop a new trusted partner relationship which will afford them opportunity to receive independent and unbiased policy compliance and data retention audits that reflect appropriate due diligence in the eyes of the court.
- Institutions completing an 80% or greater Phase 3 compliance audit will receive the **iXP System Assurance Integration Framework® (SAIF) Certification** in recognition of their level of compliance and independently audited Information Governance Assurance Program.

¹² The Sedona Guidelines: Best Practice Guidelines & Commentary for Managing Information & Records in the Electronic Age, 2007, <http://www.thesedonaconference.org/dltForm?did=Guidelines.pdf>

Phase 3 - Option:

While this final step is a critical component in the implementation of our comprehensive **Information Governance and e-Discovery Preparedness Program**, institutions may find unique value in requesting Phase 3 services *independent* of the Program.

At any time, the option exists to engage iXP's services for either a limited scope or a fully comprehensive digital holdings audit.

This iXP option may serve to:

- Provide you with a quick view of the current level of vulnerability within a particular area of interest.
- Help to gain insight into the true size of your institution's total "digital footprint".
- Serve as a "wakeup call" to key information, administration, and legal stakeholders.
- Estimate up front in dollars, the total e-Discovery cost profile of your institution's digital holdings.
- Judge the overall value of embarking on the comprehensive **iXP Information Governance and e-Discovery Preparedness Program** through a service sampling.

V. Conclusion

Today's leaders face technology challenges never before presented to their predecessors.

Leadership in today's world means increased responsibilities which now include providing guidance in new ways of thinking and operating, streamlining and controlling information repositories, and improving the litigation responsiveness of the institution's digital information.

As a partner in your quest for excellence, iXP will provide institutions with targeted solutions to identify and mitigate gaps and vulnerabilities with regard to **Information Governance** policies, procedures, enforcement, and pre-litigation preparation capabilities.

Plain and simple, the **iXP Information Governance and e-Discovery Preparedness Program** is designed to raise your institution's level of excellence in an ever-expanding digital world.

iXP – Problem Solved.