The MEARIE Group
The Reciprocal
Insurance, Financial & Business Solutions
October 2016

# Considerations for Contracts with IT Service Providers

Please be advised: the following is provided for your information only and is not intended as a statement of coverage. Insurance coverage will be determined on a case-by-case basis, nor can this response be interpreted as a legal opinion. The language, statements and phrases provided below are only for your consideration; they have not been reviewed by legal counsel and should be fully reviewed by your legal counsel before implementation. Consideration should be given that all contracts be reviewed by your legal counsel.

As with any contract, the clauses, wordings or phrases used in any agreement will depend upon the type of service being provided by the given Service provider. With IT Service contracts, your company is potentially entrusting a third party to protect your sensitive data and IT systems through which you are upholding privacy responsibilities. Contracts should be modified to meet the needs of your company as it relates to the specific services being provided.

With these types of contracts, your company's main considerations are:

1. Have your company named as an Additional Insured on the Service provider's insurance policy.
2. Your company should not be assuming the liability of others. Your MEARIE Liability policy provides coverage for your Operations Covered only, not the operations of others.
3. Ensure the contract includes standards of care in handling data and network security that are equal or better than your own company's – and ask for proof of this.

## *Insurance Considerations – Get the Service Provider to Protect You*

**Your company should be added to the Service provider's liability policy and cyber/privacy policy as an Additional Insured as it relates to the services being provided by the Service provider.**
The Service provider's insurer should provide 30 day notification of cancellation or policy change. Request a certificate from the service provider as proof of this.

**Your company should require the Service provider to have insurance in place that covers Privacy, Liability and Network Security Liability at a minimum equivalent to the coverage provided by Endorsement #8 Privacy, Cyber and Network Security Liability Endorsement of your MEARIE Liability policy.**

Coverage should provide a $10,000,000 limit for Privacy, Liability and Network Security Liability related to **Data Breach Expenses** and sums the insured may become legally obligated to pay as compensatory damages. Data Breach Expenses means those reasonable and necessary expenses incurred by the Insured or which the Insured becomes legally obligated to pay:

a) to retain third party computer forensics services to determine the scope of a failure of Network Security;
b) to comply with Privacy Regulations, including but not limited to the notification provisions of Privacy Regulations of the applicable jurisdiction that most favours coverage for such expenses;
c) to voluntarily notify parties whose Personal Information has been wrongfully disclosed;
d) in retaining the services of a public relations firm, crisis management firm or law firm for advertising or related communications solely for the purpose of protecting or restoring the Insured's reputation as a result of a failure of Network Security;
e) to retain the services of a law firm solely to determine the Insured's indemnification rights under a written agreement with an independent contractor with respect to a failure of Network Security and actually or allegedly committed by such contractor; and
f) for credit monitoring services of parties whose Personal Information has been wrongfully disclosed.

## *Indemnification & Hold Harmless Agreement*

An Indemnification Clause or a Hold Harmless Agreement in a contract may be one of the most important and often overlooked clauses, potentially having a profound effect on your company. In a contract, an indemnity clause is a legally enforceable agreement whereby one party agrees to accept the risk (assume financial responsibility) of loss another party may suffer in a specific situation. Generally an indemnity clause is looking to make the party best able to manage a particular risk responsible for the consequences of the risk materializing[1].

Basically an indemnity is just an agreement to cover the loss and damage suffered by another. It is a provision in a contract under which one party (or both parties) commit to compensate the other (or each other) for any harm, liability, or loss arising out of the contract.

The Service provider should always agree to defend and indemnify your company and its employees, directors, officers, agents, volunteers against liability for personal injury or property damage arising out of the Service provider's performance under the contract. If the Service provider will not accept an indemnification clause, this should be a red flag and your company may wish to reconsider entering into a contractual relationship with the company.

**Don't accept any sort of language in a contract that includes or requires your company to assume the liability arising out of the operations of the Service provider**. The Service provider should be responsible for their own actions and liability arising from them. The Service provider should be agreeing to indemnify your company, if the Service provider causes a loss to your company.

**A Hold Harmless Agreement** is the provision in a contract that requires one contracting party to respond to certain legal liabilities of the other party. It is recommended that a "limited form" or an "intermediate form" hold harmless clause be accepted.

**Limited Form Hold Harmless** – Where the Service provider holds your company harmless from suits arising out of the Service provider's sole negligence. Your company is thus protected when it is held vicariously liable for the actions of the Service provider.

[1] Bridge, Matthew. "Indemnities in commercial contracts – more than just boilerplate." *Hall & Wilcox*. LEXOLOGY Newsfeed. 30 May 2014. Web. Oct. 2016.

**Intermediate Form Hold Harmless** – Where the Service provider holds your company harmless for suits alleging sole negligence of Service provider or the negligence of both the Service provider and your company.

**Indemnification Hold Harmless Agreement Sample Wording:**
The following is a sample of an Indemnification Hold Harmless Agreement contract wording. (Consideration should be given that all contracts be reviewed by your legal counsel.):

> *Service provider shall defend, indemnify and hold harmless your company, subsidiaries, affiliates and their respective officers, directors, employees, agents, and successors (each of your company's Indemnitees) from and against all losses, damage, liabilities, deficiencies, actions, judgments, interest, awards, penalties, fines, costs or expenses of whatever kind, including reasonable legal fees, the cost of enforcing any right to indemnification here under and the cost of pursuing any insurance providers, arising out of or resulting from any third party claims against your company Indemnitee arising out of or resulting from Service provider's failure to comply with any obligation under this contract.*

Generally, liability insurance policies cover the operations of the Insured and do not provide for the assumption of liability under a contract, without charging additional premium and scheduling the contract. When reviewing and analyzing various contract offers from potential Service providers, it is important to consider the indemnification clause that is being provided by each.

**The Potential Cost for Indemnification**
Ensure that your company is considering the financial responsibility being transferred to the Service provider and realize that this is part of what should be built into the fee structure of the contract. If a Service provider is willing to accept the financial responsibility - through the indemnification clause you are asking them to assume - there will be an increased cost. A Service provider offering a lower bid may not be prepared to accept or take on the liability. Not all offers are equal and not all indemnification clauses are equal. Understand that you get what you pay for, not necessarily what you ask for.

## *Set the Bar High for a Standard of Care*

**Will the Service provider have access to your company's Customer data, personal information or other data that could create a privacy breach issue?**
As part of an agreement with Service providers it is recommended that, at a minimum, the agreement requirements follow your own corporate IT policies and procedures related to privacy and network security and are equal to your own standards.

**During the terms of the contract, the Service provider is responsible for the privacy and security of all of your company's data and customer information.** The Service provider needs to demonstrate their understanding of how:

1. They represent and warrant its collection, access, use, storage, disposal and disclosure of your company's data and customer personal information
2. It will comply with all federal and provincial privacy and data protection laws, as well as all other applicable regulations and directives.

At a minimum the Service provider's controls for the protection of your company's data and customer information shall include:

- Limiting access to data and information to authorized individuals
- Securing all facilities, data centres, hard copy files, servers, back-up systems and data processing equipment including but not limited to all mobile devices and other equipment with information storage capabilities
- Implementation of network device, application, database and platform security
- Securing information transmission, storage and disposal
- Authentication and access controls within media, applications, operating systems and equipment
- Encryption of highly sensitive data and customer information stored on mobile media
- Encryption of highly sensitive data and customer information transmitted over public or wireless networks
- Strictly segregating your company's data and customer information from Service provider's or other customers so that your company's data is not co-mingled with any other types of information or data
- Implementing appropriate personal security and integrity procedures and practices included but not limited to background checks consistent with applicable laws
- Provide Service provider's employees with privacy and information security training

**The Service provider needs to agree to Security Breach Procedures that protect your company. Pursue agreement that the Service provider shall do the following in the event of a security breach involving your data/systems:**

- Provide your company with the name and contact information for an employee of the Service provider who shall serve as your company's primary security contact and shall be available to assist your company 24 hours per day, 7 days per week, as a contact in resolving obligations associated with a security breach.
- Notify your company of a security breach as soon as practicable, but no later than 24 hours after Service provider becomes aware of it.
- Immediately following the Service provider's notification to your company of a security breach, both parties shall coordinate with each other to investigate the security breach in accordance with the Service provider's standard policies and procedures, a copy of which has been provided to your company.
- Take reasonable steps to immediately remedy any security breach and prevent further security breaches at the Service provider's expense in accordance with applicable privacy rights, laws, regulations and standards.

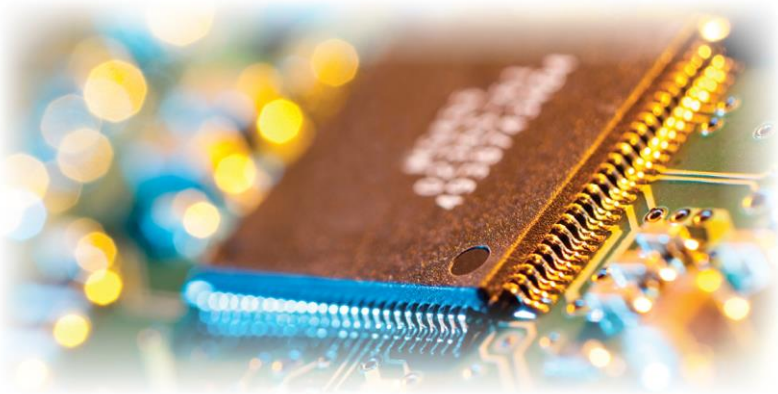
- Reimburse your company for actual costs incurred by your company in responding to and mitigating damages caused by a security breach, including all costs of notice and/or remediation.
- Agree that it shall not inform any third party of any security breach without first obtaining your company's prior written consent, other than to inform a complainant that the matter has been forwarded to your company's legal counsel. Further, the Service provider agrees that your company shall have the sole right to determine:

    (i) whether notice of the security breach is to be provided to any individuals, regulators, law enforcement, consumer reporting agencies or others as required by law or regulation or otherwise in your company's discretion; and
    (ii) the contents or such notice, whether any type of remediation may be offered to affected persons and the nature and extent of such remediation.

- Fully cooperate with your company in any litigation, claim or other formal action deemed necessary by your company to protect its rights relating to the use, disclosure, protection and maintenance of your company's data and customer information.

Entrusting another company with access to your electronic environment or with handling your data is a serious step. Ensuring your company is protected in as many ways as possible is of the utmost importance. Hopefully the information here has given you some ideas for how to develop and maintain some of the main protections.

The MEARIE Group is pursuing the goal of advancing risk management capabilities and providing risk solutions, developed specifically for the risks of the electricity sector. As an advocate for proactive risk management programs, we are your ally for support on practical risk management solutions and intelligence.





The MEARIE Group

**Gary Durie**, *Manager*
*Risk Management & Underwriting Services*
**905.265.5355 | 1.800.668.9979**
3700 Steeles Avenue West, Suite 1100
Vaughan, Ontario L4L 8K8
gdurie@mearie.ca | mearie.ca