Technology Contracts For COVID-19 **Checklist**

SNYDERMAN LAW GROUP
we support. you grow.

Internal Technology Assesments

- □ Identify and list software products that were licensed during the past six months in response to COVID-19?
- □ Identify and list products that have been licensed across the entire enterprise over the past year?
- □ What licenses have been purchased but not deployed? Are there additional licenses available?
- □ Determine if any recently licensed cloud products can replace older software products?
- □ Which employees are using which products? Are there internal authorizations in place?
- □ Is there overlap among products that have been licensed during the pandemic?
- □ Are all currently licensed products necessary for when some employees return onsite?
- □ Are security measures implemented to address working from home adequate?
- □ Are firewalls in place?
- □ Has new equipment been purchased or leased? Is there overlap? Have current leased expired or are expiring?

Technology Contract Assesments

□ For equipment leases, has the company increased its volume & license usage? Is there opportunity to renegotiate volume pricing & offset against additional or new purchases?

□ Are there multiple agreements in place with the same vendor? Can agreements be subsumed? Is there an opportunity to negotiate a more favorable master agreement?

□ If different offices/business units licensed the same product without consultation, are there inconsistent agreements? Do certain agreements contain more favorable terms?

□ If there are overlapping agreements, or the company has entered into multiple vendor agreements for competing products, what are its termination rights?

□ How are support and maintenance delivered? How have products performed during the crisis? If there have been issues, has the vendor been responsive?

□ For cloud products and services, what are the vendor's uptime policies? If the online software is unavailable, does the company receive any remedies? What are its risks?

□ What are the vendor's security policies? Have there been issues? Have other companies reported breaches? Has the vendor been responsive? What are the company's rights & obligations in the event of a security breach?

□ Do agreements contain vendor audit rights? If so, are they enterprisewide? How frequently may the vendor conduct audits, and what are the company's potential liabilities?

□ Does the company have the right to conduct its own audits of the vendor?

□ What warranties and indemnities does the vendor offer? Is liability capped? Is it mutual?

License Overlap & Overload

□ First, compile a comprehensive list of ALL software and subscription technology for which the company has active licenses & subscriptions to date. This should include:

- Enterprise wide server-based licenses
- individual user licenses
- software as a service subscriptions (SaaS)

□ Next, identify the users (individual employees, contractors, business units, offices, enterprisewide)

□ How and why is this software/subscription technology being used? And the volume of use?

□ Is this necessary in a post COVID-19 world?

□ Will the company revert to the way it was using software being COVID-19? Or will it retain some or all of its new virtual office even after employees return?

□ Once the company identifies redundancies and/or technology products no longer useful, a *technology attorney* will be able to review applicable vendor agreements.

□ If different business units/locations of the company entered into multiple agreements with the same vendor, were some negotiated while others were not? If some agreements contain more favorable terms, will the vendor consider applying those terms to all agreements for consistency?

□ Would the vendor consider subsuming the existing agreements into one master with negotiated terms and/or volume pricing incentives?

Performance, Support and Security

□ IT Department should review the frequency of support tickets, new releases and overall performance of all active software products of the past six months - prior to COVID19, during office closure in the first months of reopening.

□ IT Department should consider including stakeholders in its overall assessment by surveying various groups, office locations and levels of seniority for feedback of both new and existing technology

□ For new technology, was it accessible and user friendly? Did it deliver the promised functionality?

□ While errors and downtime are expected in cloud environments, were these situations manageable?

□ Was the company's pre-COVID-19 technology nimble enough to communicate and respond in a virtual environment?

□ If there were security breaches, how extensive were they? How quickly did the affected vendor respond? What was done to remedy the breach?

□ If the company failed to function in accordance with documentation, what rights does the company have under warranties, support or breach of contract?