

CHECKING IN ON YOUR IP PORTFOLIO

IP Portfolio







HELPFUL CHECKLIST TO ENSURE YOU TAKE PROPER STEPS TO PROTECT YOUR BUSINESS IP

- * If your business is actively developing new and innovative products, technologies, and brands, you likely have a portfolio of intellectual property assets that need to be sustained and protected.

The following checklist provides key points and tips that your business can use to help protect your IP portfolio.








PATENTS (CHECKLIST TO HELP PROTECT YOUR INVENTIONS)

-  ___ Establish a policy that prescribes how new data and ideas are to be recorded and tracked on a routine basis.
-  ___ Develop an internal disclosure system to bring new discoveries to the attention of technology supervisors and legal counsel.
-  ___ Review new technology regularly to identify features that can provide a competitive advantage, if kept exclusive. If these features are new and inventive, file an initial patent application.
-  ___ In view of the potential world-wide market, consider filing a foreign or international patent application within a year of each priority application.
-  ___ Periodically review pending patent applications to reallocate expenditures to newer technology, when appropriate.
-  ___ Periodically review matured patents to identify protected but unused technology that can be licensed out as an additional source of revenue.

CHECKING IN ON YOUR IP PORTFOLIO



IP Portfolio

TRADEMARKS (CHECKLIST TO PROTECT YOUR BRAND)

-  — Before committing to a new product name or logo, consider commissioning a trademark search to avoid names and designs already used by other companies.
-  — Develop a compelling image for your products and services by having a structured process to create the names used by your business, advertising slogans, packaging, advertising, and website design.
-  — File a trademark application for each brand name, logo, and product ornamentation that identifies or has come to distinguish what your company sells.
-  — Consider whether licensing a trademark to another company may help promote the brand or increase your market share.
-  — Periodically conduct quality control audits on products and services sold under the trademarks you have licensed to others.




TRADE SECRETS (CHECKLIST TO PROTECT SENSITIVE CORPORATE POLICIES, PROCEDURES AND INFORMATION)

-  — Establish an internal policy to identify and safeguard trade secrets (such as underlying technology, unpublished patent applications and data, ideas, know-how, computer code, and customer lists).
-  — Have confidentiality and non-compete agreements with business partners, potential business partners, contract employees, consultants, visitors, and others who may have access to your trade secret information.





CHECKING IN ON YOUR IP PORTFOLIO

IP Portfolio

-  ___ Establish a chain of authority for approving publication or other public disclosure of your technology. Have written agreements with your business partners about the publication and patenting of joint inventions.




COPYRIGHTS (CHECKLIST TO PROTECT YOUR CREATIVE WORKS)

-  ___ Secure the necessary registration for your website, written works, specific designs, specific graphics, etc. to help mitigate the risk of direct copying by competitors.
-  ___ Utilize the “©” symbol, the name of the author, and date of the work on each piece of original material, including advertisements, catalogs, web pages, unique product designs, graphics, and so forth.
-  ___ Require employees to assign the legal rights to any original works created during the course of their employment to the company and declare such works were created as “works for hire.”
-  ___ Require outside designers to assign the legal rights to any original works created while completing a project to the company and declare such works were created as “works for hire.”






DOMAIN NAMES

-  ___ Register or acquire a cadre of domain names that reflect not only your company name, but also branded products, trademarks, and derivative names.

CHECKING IN ON YOUR IP PORTFOLIO

IP Portfolio

-  ___ Empower your public affairs and marketing group to take charge of your company's presence online so that the site reflects your company's brand.
-  ___ Have a Terms of Use section that indicates IP rights owned by the company, acknowledges third-party trademarks, and includes disclaimers and limitations appropriate for the products and services you provide.
-  ___ Have a Privacy Policy section informing users about how you collect and use order information and other data from the site.












DATA PRIVACY (CHECKLIST TO HELP ENSURE YOUR CORPORATE YOUR CORPORATE DATA IS NOT INADVERTENTLY RELEASED OR HACKED)

-  ___ Establish a data mapping protocol to ensure key data points are properly maintained and managed.
-  ___ Determine if your business needs to comply with specific state data privacy regulations and/or international data privacy regulations such as the GDPR.
-  ___ Implement a clear, understandable protocol for an individual to opt out of selling personal information.
-  ___ Develop a system that will allow your business to efficiently manage the individual rights of disclosure, access and deletion of personal data.
-  ___ Monitor and track U.S. privacy laws since more states are considering enacting new privacy regulations that mirror California's privacy framework.

CHECKING IN ON YOUR IP PORTFOLIO

IP Portfolio

CYBERSECURITY (CHECKLIST TO HELP PROTECT SENSITIVE DATA AND INTERNAL OPERATING SYSTEMS)





-  __ Establish a detailed Incident Response Plan (IRP) in the event of a cyber breach.
 -  __ Invest in employee training and awareness programs (this is due to the fact that the majority of cyber incidents are caused by employees inadvertently clicking on phishing e-mails)
 -  __ Implement internal password policies to ensure any new passwords are sufficiently complex.
 -  __ Require employees to periodically update their passwords to improve security and inadvertent access to internal databases.
 -  __ Utilize Multi-Factor Authentication to provide an additional layer of security when employees access an internal database.
 -  __ Update operating systems and antivirus programs to strengthen internal security measures.
 -  __ Use filtering software to help mitigate the risk of phishing e-mails.
 -  __ Ensure data is backed up on a regular interval to mitigate the risk of unnecessary loss.
 -  __ Invest in a cybersecurity insurance policy that covers the liabilities associated with data breaches in part or in full.
-



CHECKING IN ON YOUR IP PORTFOLIO

IP Portfolio

AFFIRMATIVELY ASSERTING YOUR IP RIGHTS (CHECKLIST ON HOW TO MAKE SURE OTHER BUSINESSES DO NOT ABUSE OR STEAL YOUR IP)

-  ___ Mark each product with the serial number of each issued patent that protects the product or its use.
-  ___ Identify all trademarks used with your products, services, packaging, promotional material, and website with the symbol ® if the mark is registered. Otherwise, use the symbol.™
-  ___ Survey competing products and services periodically to see if they are using technology covered by the claims of your patents.
-  ___ Survey competing products and services periodically in your channel of trade to see if another company is using a trademark or guise that resembles your own.



OMID E. KHALIFEH

Principal Patent Attorney
omid@omnilg.com

OMNI LEGAL GROUP

2029 Century Park East, Suite 400
Los Angeles, CA 90067

310.276.664

855 IDEA BANK
www.omnilegalgroup.com

Follow Us!    

PRIVILEGED AND CONFIDENTIAL COMMUNICATION

This electronic transmission, and any documents attached hereto, may contain confidential and/or legally privileged information. The information is intended only for use by the recipient named above. If you have received this electronic message in error, please notify the sender and delete the electronic message. Any disclosure, copying, distribution, or use of the contents of information received in error is strictly prohibited. Please consider the environment before you print this e-mail.