CWO
2 September, 2015

Guidelines
How to manage confidential information

Introduction

In today's competitive environment, all types of organizations, including research organizations, need to be as innovative as possible to prosper and to keep the pace with progress. To this end, the development and acquisition of useful information is crucial to create and provide new and improved tools and services. Information about technology that makes an organization's product unique, prototypes, or even a list of key customers are just a few examples of information that can make the difference. As the latter can have a great commercial value and significant importance for the organization concerned, its uncontrolled disclosure might potentially lead to serious consequences.

Research organizations in particular may not be aware of this risk and thus of the importance of keeping this valuable information "confidential". Indeed, such information relates to intangible assets and falls under the category of intellectual capital, but its protection is not regulated within the intellectual property rights (IPR) system. That is why confidential information belongs to the so-called **Soft IP**.

These guidelines will illustrate the importance of confidentiality for research activities and give hints on protection management of confidential business information, which could prove beneficial in particular to research organizations.

1. Confidential information and trade secrets

Confidential information is considered as information that must be kept secret. While any information can be confidential, not all the information generated within an organization must be kept secret. What is confidential is judged by the academic staff on the circumstances of each individual case, based on the necessity of it not being disclosed.
Confidential information may refer to **personal information** (e.g. journals, pictures), **professional information** (e.g. information supplied in the course of professional duties) and **information in the context of business, commerce** or **trade** (i.e. trade secrets).

For the purpose of this document, we will focus on **trade secrets.** Trade secrets are confidential information related to research. Broadly speaking, trade secrets are any confidential business information which provides an organization with an economic benefit that translates into competitive advantage, and this directly derives from the fact that the secret is generally unknown to competitors due to the efforts of its owner to keep it secret.

Trade secrets are critical to the functioning of an organization and any unauthorized or accidental disclosure of trade secrets may destroy their confidential status and may cause a considerable economic loss for the business concerned. If not protected, competitors could use this information without having to bear the costs or risks and the owner of the trade secret would certainly lose the competitiveness built on this information. Trade secrets are relevant for example when a product or process is not considered worth a patent or is not patentable at all, as well as an alternative option to patenting. Yet, they also play a fundamental role before seeking a patent. During this period in fact, disclosure of patent features may destroy patentability.

T**rade secrets require an appropriate internal management program.** Any researcher should put in place a safeguard system within its organization for protection of trade secrets to be effective. This would require **goodwill** and **maintenance,** which in some cases is the most fruitful IP protection. Indeed, a trade secret offers a **broader scope of protection** than other forms of IPR as, once the very low requirements are met, any information related to technology, design, art, marketing, idea, concept and so forth, can be protected. Moreover, trade secrets are **much cheaper** than IPR as they need no registration or any official procedure to be protected and, most importantly, as long as secrecy is kept they are **effective without time limits**. Therefore, the term of protection can be perpetual as regards trade secrets.

2. How to assess a trade secret

For information to be legally protected as a trade secret it must:

- Be unknown to the circles that normally deal with that kind of information;
- Confer some sort of economic benefit because it is secret;
- Be the result of reasonable efforts to maintain its secrecy.

In deciding what's confidential, look at:

- the extent to which the information is known externally
- the extent to which the information is known by employees and others involved
- the value of the information to competitors
- the amount of effort or money expended in developing the information
- the ease or difficulty with which the information could be properly acquired or duplicated by others

Some information qualifying as a trade secret:

- ✓ Information relating to formulas, patterns, devices or other compilation of information that is used for a considerable period of time (e.g. Coca-Cola recipe);
- ✓ Technical information used in the manufacturing process for production of goods, including software used for various purposes (e.g. the ZARA's IT system to shorten the production cycle);
- ✓ Marketing, export or sales strategies, or a method of bookkeeping or other management routines or procedures (e.g. list of key suppliers and/or buyers).
- ✓ Other information may include financial information (e.g. business plans, purchase prices of key raw materials, list of key customers, product specifications, test data, technical drawings or sketches, engineering specifications, contents of workbooks, the salary structure, any kind of agreement, promotional or marketing material under development).

3. Trade secrets protection management

3.1. Identification of trade secrets

To start with, a strategic assessment of the organization's valuable research information is a prerequisite to set a protection program. To identify trade secrets, two fundamental questions should be asked:

- **Does the information bring any economic benefit to my organization?**
- **Would its leak hurt my activities?**

Define as much as possible the type of information that you are trying to protect!
If you decide to have a confidentiality policy, you need to specify exactly what you're protecting and what you consider confidential in order to prevent current or former employees from later claiming that they did not realize that the information they were using, sharing, etc., was protected.

Making a list of all this information and organizing it into different sections, depending on its value, will help to understand the type of measures to take for its protection to be effective. Once academic staff of a department has evaluated that its activity relies on an amount of valuable know-how, it should set a protection policy to provide clarity (particularly to its employees) on all the aspects that need to be addressed. It is very important to define how information should be revealed and how it can be shared within and outside the department. It is also advisable to provide a list of the information not covered by confidentiality.

3.2. Safe handling, storage and disposal of confidential information

See Annex 1

3.3. Employee awareness

To avoid your business or research strategy being disrupted, employees should be aware of the organization's security policy and their duty with regard to confidentiality, as well as the consequences of a breach of such duty.

3.3.1. Employee training

Employee education is fundamental to handling trade secrets. Training on information security allows the establishment of a culture of information security within the organization and is perhaps the most profitable aspect of confidentiality management.

3.3.2. Non-disclosure clauses

Although in most EU countries it is not necessary to sign a separate confidentiality agreement due to the national labor laws that require a confidentiality duty on the employees, it is highly recommended that strong contractual provisions be foreseen. This is the case of **non-disclosure clauses** within employment contracts that oblige employees not to use trade secrets acquired in the course of the employment.

Confidentiality clauses should clearly state:

- The information to which the obligations apply;
- The specific obligations and restrictions imposed on the recipient;
- The consequences of breach of confidentiality;
- The obligations to be applied after termination of their employment with the organization.

3.3.3. Non-compete agreements

Employees leaving the organization are a source of expertise (i.e. knowledge, skills, and experience) acquired therein. While the latter cannot be restricted, signing **non-compete agreements** would ensure that trade secrets acquired during the employees' duties are safeguarded for a certain period of time after their departure. More precisely, these agreements would require a former employee not to work for a direct competitor up to the time when the secret information loses its inherent value to the business.

3.3.4. Document marking

Although employees are under a confidentiality obligation**, marking documents** can prove to be crucial by allowing employees to properly treat the documentation, avoiding incurring liability, and mainly by making sure that information are handled in a confidential manner.
There are different ways for marking trade secret information. Some of them are:

- ✓ CONFIDENTIAL
- ✓ THIRD PARTY CONFIDENTIAL
- ✓ MAKE NO COPIES
- ✓ DISTRIBUTION LIMITED TO ____
- ✓ COVERED BY A NON-DISCLOSURE AGREEMENT

Each of them can be further classified as CRITICAL, MAXIMUM, MEDIUM, and MINIMUM

3.4. Partner commitment - Non-Disclosure Agreements (NDA)
When revealing sensitive information to a partner, the fact of simply attaching a confidentiality notice to the communication does not automatically create an obligation on the receiving party. The best approach to keep confidential information away from competitors is indeed to make your partners sign a Non-Disclosure Agreement (NDA). Thanks to these contracts, the recipient will be impeded in disclosing trade secrets and if a disclosure occurred, it would be liable to breach of contract and likely to be subject to financial penalties.
Since research and business information may represent a dominant factor in making prospective partners decide whether to start a new relationship, NDAs are extremely useful before disclosing any valuable information during partnership negotiations such as licensing and joint ventures.

4. Steps to manage confidential information

4.1. Identify valuable business information.
See chapter 2
Tip: Narrow down the information as much as possible.
Limiting the amount and providing a good description of the sensitive information will increase the likelihood of adequate compliance. It is, for example, much easier to protect a specific sequence than a complete thesis.

Keep in mind that recent policy measures are stimulating Open Science, Open Research, and Freedom of information for Government and Public institutes. Further tightening can be expected.

> *Open Science (Open Access)*
> *Science and research have always been open, but some of the processes for producing research and disseminating its results are not.*
> *The global shift towards giving free online access (**open access**) to the results of publicly-funded research (publications and data) has been a core strategy in the European Commission to improve knowledge circulation and thus innovation. It is illustrated in particular by the general principle for open access to scientific publications in Horizon 2020 and the pilot for research data. It is now widely recognized that making research results more accessible to all societal actors contributes to better and more efficient science, and to innovation in the public and private sectors. In 2012, via a Recommendation, the European Commission encouraged all EU Member States to put publicly-funded research results in the public sphere in order to strengthen science and the knowledge-based economy.*
> *The European Commission is now moving beyond open access towards the more inclusive area of **open science**. Elements of open science will gradually feed into the shaping of a policy for Responsible Research and Innovation and will contribute to the realization of the European Research Area and the Innovation Union, the two main flagship initiatives for research and innovation.*

4.2. Design a protection management policy.
See Annex 1 (Best practices for dealing with confidential data)
See Annex 2 (Best practices Masterproef)

4.3. Decide who needs to deal with the information (need to know, not nice to know).
Staff, students (internal, exchange), partners (internal, external)

Make sure that the necessary agreements with involved stakeholders are completed.

- ✓ Non-disclosure agreement: http://www.techtransfer.ugent.be/en/support-for-academics/legal-support
- ✓ Overeenkomst Masterproef: http://www.ugent.be/nl/onderzoek/maatschappij/overeenkomstmasterproef.pdf
- ✓ Overeenkomst masterproef voor gaststudenten: https://www.ugent.be/student/nl/administratie/inschrijven/gaststudentugent/gaststudentmasterproef.pdf
- ✓ Master dissertation contract: http://www.ugent.be/nl/onderzoek/maatschappij/masterdissertationcontract.pdf
- ✓ Eenzijdige vertrouwelijkheidsverklaring student: http://www.ugent.be/nl/onderzoek/maatschappij/eenzijdigeverklaring.pdf
- ✓ Unilateral declaration student: http://www.ugent.be/nl/onderzoek/maatschappij/masterdissertationcontract.pdf

4.4. Provide training to involved stakeholders to ensure compliance.

Annex 1

BEST PRACTICE OFFICE PROCEDURES FOR DEALING WITH CONFIDENTIAL AND REGISTERED CONFIDENTIAL DATA

This document is intended to provide guidance to individuals (including faculty staff, graduate assistants, student employees, and others) and departments dealing with data that the University classifies as "confidential".

Computers and Printers:

When possible, computers and printers that might be used for confidential data should be placed in secure areas where access is restricted to only those individuals with permission to access confidential information.

Stand at public printers or have documents containing confidential information retrieved immediately so that unauthorized individuals have no opportunity to see the information.

Computer Display:

Remove confidential data from screens where it is not required.

Be aware of the position of computer screens. Unauthorized individuals should not be able to read screens containing confidential information. Use a monitor visor or hood in service areas.

Be sure to log off from applications that show confidential data so that no data is accessible after you are finished.

Computers that are used to access confidential data should have screen savers so that unauthorized people cannot read the information if they happen to wander into a restricted area.

Computers that are used to access confidential data should have a time-out feature so that when a staff person steps away from his/her computer for a period of time, the staff person is required to re-enter his or her password.

The use of a password protected monitor is highly recommended.

Telephone, Internet (email) and Other Communications:

Limit information that is to be provided to others to what is required/needed/requested. Do not use a general form that contains additional confidential information not required to satisfy a request. For example, if another office needs to verify name and address information, and that information appears on a form that also contains other confidential information either black out the unnecessary information on the form or else use another means for providing the requested information.

Conversations (between staff members and/or staff and other individuals) containing confidential information must be restricted to ‘private’ and non-traffic areas where the conversations cannot be overheard by others. When reasonable, move to a private room, move to a corner of a room, keep voices low, etc.

Avoid discussing confidential information in public spaces such as elevators or cafeterias.

Never ask an individual to speak confidential information in a public setting. Ask the individual to write it on scrap paper (which is then returned to the individual) or to key it on a keypad for input to the computer.

When acquiring confidential data via telephone, ask "Are you in a private location where you can give me your confidential information verbally"? Also, never repeat information provided so that others can identify the individual with whom you are speaking and hear details of their information.

Verify the identity of individuals to whom you are providing confidential information. Do not disclose confidential information to unauthorized individuals (including family members and friends) unless the affected person has given permission. Follow any additional procedures established by the data custodian for that data.

Never leave voice mail messages containing confidential data.

On voice mail boxes that may be accessed by more than one individual, leave instructions on the voice mail that instructs the caller not to leave confidential information as part of their message.

Follow procedures developed by your departments for accepting confidential information from outside your department and ensuring the confidentiality of that information that is received by your department. These procedures should include handling of email messages containing confidential information.

Paper:

Do not use sign-in sheets that contain confidential information. In some cases even having full names on a sheet that is available to others might be considered breaching confidentiality. Limit sign-in sheets to first name only.

Do not post lists containing confidential information, nor have such lists in a place which can be viewed by others.

Remove confidential data from reports where it is not required.

Paper records and reports containing confidential and sensitive information must never be left in locations where non-staff individuals (or others without authority to view the information) have access to that information such as printers or unattended on a desktop in open view. Reports which are no longer needed and which contain confidential and/or sensitive data, must be shredded or stored securely until it can be shredded or processed for recycling.

Account for any lists, records and reports containing confidential information that are used during conferences or other meetings. Do not leave materials in meeting rooms.

Labeling:

All confidential documents should be labeled appropriately with the highest classification level that pertains to the document (confidential, internal use only). All draft documents should be clearly labeled as such.

Disposing of Materials containing Confidential Information:

Observe retention guidelines in selecting documents to be destroyed.

Records transferred to the archives which are considered confidential should be accompanied by a statement specifying: (1) the persons or administrators allowed to use the records, and (2) the length of time the records should be treated as confidential.

Confidential information not subject to records retention policies that is no longer required for business reasons should be discarded in a secure manner. Paper should be shredded prior to disposal and shredding bins should be emptied on a regular basis. Microfiche copies should be shredded or burned. Electronic information (hard disk, CD, etc.) must be destroyed, either by re-initializing (for Macs), or by using data wipe software or a degausser, or by physically destroying the media on which it is maintained.

Erase recording tapes (from dictaphones or recorders); not just writing over them.

Never dispose of printed confidential information in a regular trash container.

Passwords:

Computers that are used to access confidential data must be password protected.

Employee should only be given access to those computers and information to which they are entitled. Each employee must use his/her own password to access computers containing confidential data. Passwords need to be kept confidential (not shared with anyone else) and need to be changed on a regular basis to ensure security. Passwords must never be left on "Post-it" notes next to the computer.

Laptops and PDAs:

Unless given approval by a department head or other designated authority, laptops or other portable devices (PDA’s, usb sticks, etc.) should not be used to store confidential information.

Laptops and other portable equipment that contain confidential information must be kept secure and able to be accessed only by authorized individuals.

Delete confidential information from laptops and personal devices as soon as it is no longer needed on those devices.

Personal (Home) Computers:

Home computers that can be accessed by other individuals (family members and/or friends) should never be used to store confidential university information. Even when the computer is not used by others, prior approval must be granted by the custodian of the data before downloading and/or storing confidential university information. Where approval is granted, the same security standards used for work machines must be used with the home computer.

Storage of confidential information:

Store copies of confidential information, such as printouts, in locked file cabinets or desks.

Store non-reproducible confidential information in areas designed to safeguard it from unauthorized viewing and damage from natural cause.

Store portable equipment in a locked file cabinet or desk.

Administrative data should be stored on the network drive rather than physical drive on your PC.

Regularly back up locally maintained confidential information stored on disk to ensure that information is not lost in the event of disk failure and store backups in a locked facility with limited access.

Protect electronic records containing confidential data, including backups, during storage by encrypting the confidential data.

Place confidential data stored on a hard disk in a segment that is protected by an approved security program requiring an access password.

Keys and access cards that permit entry into storage facilities where confidential data is stored must not be loaned or left where others could use them to access the secure areas.

All confidential information must be protected from cleaning staff, maintenance staff and others who may have a need to access the facility where confidential information is located.

Records and reports (paper and electronic) containing confidential information should be stored in locked rooms, cabinets and/or desks when not in use. Access to these rooms, cabinets and desks must be limited to those who are authorized to access the confidential information.

Employees should 'clean' their desks of all materials containing confidential information prior to leaving at the end of the day, and store the materials securely.

Access

Ensure that all keys and other items that allow access to confidential information, both physical access and computer access, are returned when the individual's access to the information is no longer appropriate.

Do not look up confidential information pertaining to yourself or anyone else unless you are authorized to do so.

Limit access to confidential information to the minimum needed to do the job.

Implement electronic audit trail procedures to monitor who is accessing what.

Use logs or electronic audit trails to monitor employees' access to records with confidential data.

If you are required to share confidential data with other (third-party) organizations, including contractors, use written agreements to protect their confidentiality. Such agreements should prohibit such third parties from re-disclosing the confidential data, except as required by law; require such third parties to use effective security controls on record systems containing confidential data; require the return or secure disposal of the data when the agreement ends, and hold such third parties accountable for compliance with the restrictions you impose, including monitoring or auditing their practices.

Security Incidents

If confidential data is disclosed inappropriately and the individuals whose confidential data was

disclosed are put at risk of identity theft or other harm, initiate a security response that promptly notifies the individuals potentially affected.

Bijlage 2:

REGLEMENTAIR KADER MASTERPROEF

http://www.ugent.be/bw/nl/voor-studenten/curriculum/masterproef
http://www.ugent.be/bw/en/for-students/curriculum/master-dissertation

VERTROUWELIJKHEIDSASPECTEN VAN DE MASTERPROEF

Vertrouwelijkheidsaspecten kunnen contractueel bepaald zijn in onderzoekscontracten of vrijwaren de optie om een uitvindingsaanmelding te kunnen indienen n.a.v. resultaten die bekomen werden uit een masterproef.

De toepassing van onderstaande richtlijnen is verplicht wanneer de masterproef gerelateerd is aan onderzoek met contractuele vertrouwelijkheidsafspraken. Daarnaast kan octrooibescherming van valoriseerbare resultaten een goede reden zijn om bepaalde onderzoeksaspecten confidentieel te houden en kan een publicatie embargo ingesteld worden. De toepassing van de vertrouwelijkheidprocedures gedurende de uitvoering van de masterproef belet echter niet dat finaal publiekmaking van de masterproef beoogd wordt.

Richtlijnen voor een masterproef met vertrouwelijke aspecten

1. Het voorstellen van de onderwerpen door de promotor/begeleider aan student(en)

· Geen vertrouwelijke informatie vermelden.
· Aangeven of de masterproef al of niet in samenwerking is met een bedrijf (indien in samenwerking met een bedrijf kan een publicatie embargo van 10 jaar ingesteld worden, dit is evenwel aanpasbaar, zie #8).

2. Het toelichten van onderwerpen door de promotor/begeleider aan student(en)

· Geen vertrouwelijke informatie meedelen aan de student (dit kan vanaf #3).
· Studenten attent maken op de overeenkomsten betreffende de masterproeven.
· Voor inkomende Erasmus-studenten is het af te raden om een onderwerp aan te bieden met vertrouwelijkheidsaspecten aangezien het moeilijk is om te controleren of de masterproef publiek gemaakt wordt in de thuisuniversiteit.

3. Opstartvergadering masterproef door promotor/begeleider/student

· De student de vertrouwelijkheidsverklaring laten ondertekenen.
· De promotor maakt de vertrouwelijkheidsverklaring over aan FSA.

4. Begeleidingscommissie [promotor/begeleider]

· Niet-UGent-medewerkers in de begeleidingscommissie ondertekenen de vertrouwelijkheidsverklaring.
· De vertrouwelijkheidsverklaring wordt door de promotor overgemaakt aan FSA.
· UGent-medewerkers worden door de promotor duidelijk op de hoogte gebracht van het vertrouwelijk karakter van het onderzoek. Leg de precieze vertrouwelijke elementen vast.

5. De uitvoering van de masterproef door de student

· Met respect voor de vertrouwelijkheid (zie Annex 1).
· Weet dat studenten mee opgenomen kunnen worden op een UGent-uitvindingsaanmelding.

6. Begeleiding van de masterproef door de promotor/begeleider

· Bewaak de vertrouwelijkheidsaspecten die contractueel afgesproken zijn in de onderzoeksovereenkomst waarop de masterproefstudent werkzaam is.
· Overweeg een uitvindingsaanmelding alvorens iets publiek te maken (www.techtransfer.ugent.be > support for academics). Je kan steeds ruggespraak houden met de business development managers van UGent en de techtransfer-adviseurs.

7. Tussentijdse verdediging [promotor/begeleider/student]

· Vertrouwelijkheid resulteert in een 'gesloten' tussentijdse verdediging (alle aanwezigen zijn gebonden door vertrouwelijkheid, zie #3 en #4).

8. Goedkeuring van de titel en de beoordelingscommissie en beslissing over een publicatie embargo door de promotor/begeleider

· De titel mag niet confidentieel zijn en mag daarom geen vertrouwelijke informatie omvatten.
· In functie van de vertrouwelijkheidsaspecten (in welke mate er confidentiële informatie wordt opgenomen in de masterproef, in welke mate contractuele bepalingen van toepassing zijn, in welke mate octrooibescherming is genomen) stelt de promotor een eventuele embargodatum in.
· Niet-UGent-medewerkers in de beoordelingscommissie ondertekenen de Vertrouwelijkheidsverklaring (zie 4.3).
· De vertrouwelijkheidsverklaring wordt door de promotor overgemaakt aan FSA.

9. Finaal document van de masterproef [student]

· Indien beslist wordt door de promotor/begeleider dat de masterproef vertrouwelijk moet blijven (voor een bepaalde duur), worden de vertrouwelijkheidsaanduidingen mee opgenomen zoals aangegeven bij de richtlijnen 'Vorm van de masterproef'.
· Op het titelblad van de masterproef moeten de vertrouwelijkheidsaanduidingen opgenomen worden.

10. Pdf van de masterproef opladen in MINERVA

· De student laadt de pdf op in MINERVA en vinkt 'confidentieel' aan, zodat een eventueel embargo op publicatie wordt ingesteld conform UGent richtlijnen (zie #13).

11. Hard copy voor de beoordelingscommissie

· De papieren versie wordt gemarkeerd als zijnde vertrouwelijk (zie #9) en wordt als dusdanig (zie Annex 1) bewaard door juryleden/promotor/begeleider/student.

12. Eindverdediging

· Een vertrouwelijke masterproef resulteert in een 'gesloten' verdediging (alle aanwezigen zijn gebonden door vertrouwelijkheid, zie #3, #4 en #8).

13. Opname van de masterproef in de digitale bibliotheek

· Na deliberaties worden de masterproeven automatisch opgenomen in de digitale UGent bibliotheek [≥ 10/20 open voor UGent, ≥ 14/20 open access, tijdens een embargoperiode zijn masterproeven niet zichtbaar].