Code of Ethics and Business Conduct

Last Revised : February 2025

Table of Contents

Foreword

Dear employee,

Many people contribute to the success of D-BOX, including you and your co-workers, as well as our clients, suppliers and partners. Everyone plays a crucial role and everyone has responsibilities. Mutual respect, a strong sense of duty and utmost professionalism are essential. In addition to ensuring a climate of healthy collaboration and the smooth running of our activities, our Code of Ethics and Business Conduct (the "**Code**") is intended to clarify D-BOX's commitment to you and the specifics of your commitment to the Company.

D-BOX has adopted a Code of conduct that is guided by the following 10 principles, which are easy to remember and put into practice:

1. Put the general interest of the Company first and protect our shareholders;
2. Comply with applicable laws;
3. Respect our clients and the users of our products;
4. Act fairly toward our competitors;
5. Refuse to tolerate conflicts of interest and report all breaches of the Code;
6. Refuse to tolerate any form of discrimination or harassment, and promote diversity;
7. Ensure the quality of working conditions;
8. Foster employees' personal and career development;
9. Protect the environment and employees' health and safety;
10. Show good citizenship wherever we operate.

Each member of our team is bound by this Code and is responsible for putting it into practice.
D-BOX must comply with all applicable legal requirements, while maintaining the highest standards of conduct and integrity. This entails much more than a list of standards the Company asks you to follow. First and foremost, it is a matter of behaviour, attitude and respect for oneself and others.
D-BOX is counting on each and every one of you to adopt appropriate rules of conduct, in order to maintain a healthy, stimulating work environment without constraints.

Sébastien Mailhot
President and CEO

1. Presentation of D-BOX Technologies

D-BOX Technologies Inc., including D-BOX USA Inc., as well as any other subsidiary of the Company (hereinafter collectively called the “Company” or “D-BOX”), designs, manufactures, and sells cutting-edge motion systems intended for the entertainment, simulation and training markets. Its unique, patented technology uses motion effects specifically programmed for each visual content, which are sent to a motion system integrated into a platform, seat or any other product. The resulting motion is perfectly synchronized with the on-screen action, creating an unparalleled realistic immersive experience.

In this Code, the masculine form is used, without prejudice, for the sake of brevity.

1.1 Our Vision

With D-BOX, people can become more deeply engaged with experiences, enjoying a feeling of presence that is fuller and richer than ever before.

1.2 Our Mission

D-BOX enables people to experience life in all its richness like never before.

1.3 Our Values

D-BOX has defined four (4) strategic values that guide people at every level of the Company, to acknowledge and support the organization’s uniqueness and to formalize its members’ historical and fundamental values. While each value is important on its own, they are all interconnected and share a common goal: to position D-BOX as an employer and supplier of choice on the market.

PEOPLE

Are at the heart og our growth, They’re the reason for our engagement. They embody both our corporate empathy and brand integrity.

AGILITY

It’s living proof of our evolution…the force that moves us continuously forward. It’s ever-changing offering us the freedom to adapt whenever, wherever, however.

CREATION

It’s at the heart of our organisation, It represent our ultimate end-goal, our signature; the source of all our endeavours. It unites the hearts & minds of all our artists & artisans.

GOING BEYOND

It’s our driving force. Our common motivator. It inspires us tu push our own limits…and strive to deliver our very best.

2 Application and Responsibility

The Code sets out the legal standards of conduct and ethics for the Company's staff members.

2.1 Policy Statement

This Code applies generally to all directors, officers and employees of the Company, as well as to its consultants and partners when the latter are dealing with D-BOX, acting on its behalf or as its representatives. Because a written Code cannot answer all of the questions that may arise in the context of business relationships, each person covered by this Code must take responsibility for recognizing particular situations when they arise and for responding appropriately to them. Any question concerning the requirements of this Code or the appropriateness of a relationship or action should be addressed to your immediate supervisor or the Legal Department. Questions coming from a director or an officer, including the President and CEO, should be addressed to the Chair of the Board of Directors or the Chair of the Compensation and Corporate Governance Committee (hereinafter called the "Governance Committee").

2.2 Scope of the Code

This Code applies to all employees of D-BOX, including part-time, temporary and contract employees, and consultants. It establishes the procedure through which Company employees may submit their concerns about internal practices or internal auditing issues anonymously and confidentially to the Chair of the Governance Committee of the Company's Board of Directors, without fear of retaliation.

2.3 Compliance with Laws and Regulations

All employees, consultants, officers and directors must comply and do their best to ensure that the Company complies with all applicable laws and regulations wherever it conducts business, including standards set by various securities commissions and stock exchanges in all jurisdictions where the Company's shares are traded. Good judgment and common sense should be exercised in striving for compliance and in asking for advice when uncertain about the action to be taken.

2.4 Declaration of Responsibility of the Company

D-BOX's commitment to its officers, shareholders, directors, employees and consultants is to adhere to high standards of conduct, to comply with best practices in terms of business conduct, and to comply with legislation. As such, several guidelines have been developed and compiled in this Code.

All directors, officers and managers are required to familiarize themselves with the content of the Code. Officers must also have in-depth knowledge of the Company's business practices and of the policies that directly concern their work.

Managers must take all reasonable measures to ensure that employees and other partners are familiar with and comply with the Code. They must, as needed, speak to a superior when in doubt as to the application of the Code.

Managers must also:

- ensure that all employees and consultants have access to the Company's policies and procedures;
- respond quickly to employees' or consultants' questions and concerns about business conduct, and ask for advice, if needed;
- behave in an exemplary manner, serving as a model to employees and consultants.

2.5 Declaration of Responsibility of Employees, Consultants and Officers

All Company employees, consultants and officers must adhere to this Code. More specifically, employees, consultants and officers shall:

- be committed to the Company in providing quality services, responding to requests addressed to the Company and performing their work efficiently;
- avoid any action that could cause harm to the interests, image and reputation of the Company or its clients;
- undertake to protect the confidentiality of their employment or mandate. All confidential data, information and knowledge about the Company, or produced as part of a project, or acquired during their employment or mandate, may not be disclosed to third parties or used for personal reasons without the Company's express written consent;
- undertake, at the end of their employment or mandate, to return all documents, reports, notes, electronic files or other item produced as part of their employment, the latter being the exclusive property of the Company;
- undertake to consult, as needed, their manager, the Legal Department or Human Resources about any information in this Code whose meaning or application is unclear.

2.6 Duty to Report Breaches

Every employee, consultant, officer and director has a responsibility to ask questions, seek advice, report suspected breaches and express concerns regarding compliance with this Code or any other Company rule. Any person who believes that another employee, consultant, officer or director is engaging or about to engage

in conduct that violates applicable legislation or this Code should promptly communicate this information to the Legal Department or to the Chair of the Governance Committee.
Section 2.9 of this Code covers “Reporting and compliance procedures” related to whistleblowing.

2.7 Breach of the Code

Failure to comply with the standards set by this Code or any other policy of the Company shall result in disciplinary action, possibly including, but not limited to, reprimands, warnings, periods of probation or suspension without pay, demotion, salary reduction, dismissal or withdrawal and rehabilitation. Certain violations may be reported to public authorities for investigation or legal proceedings. Moreover, any supervisor who orders or approves any conduct whatsoever that violates this Code or any policy, or who has knowledge of such conduct and does not report it promptly, shall also be subject to disciplinary action, up to and including dismissal.

2.8 Exemptions from the Code

While certain rules in this Code must be strictly adhered to without fail, exceptions are possible in other cases.

Any employee or consultant who believes his situation requires an exception to the Code should first contact his immediate supervisor. If the latter deems an exception to be appropriate, the final approval of such exception by of the President and CEO must be obtained. The President and CEO may discuss the matter with the Legal Department before approving the exception.

Any officer or director seeking an exception to this Code should submit his request to the President and CEO or to the Chair of the Governance Committee. Only the Board of Directors, on the recommendation of the Chair of the Governance Committee, may grant an exemption from this Code to an officer or a director; such exemption shall be publicly disclosed when required by law.

2.9 Reporting and Compliance Procedures

Any person who believes that another employee, consultant, officer or director is engaging or about to engage in conduct that violates applicable legislation or this Code should promptly communicate this information to the Legal Department or to the Chair of the Governance Committee. It is also possible to report such conduct anonymously; however, there may be circumstances in which the Company could be forced to reveal the whistleblower's identity.

The Company may not punish, discriminate or retaliate against any person who may report such conduct in good faith or who cooperates in any investigation or inquiry into such conduct.

The Company's Legal Department shall keep written records of all reports of significant breaches of this Code and their resolution, as well as all exemptions from this Code that are granted.

The Governance Committee shall periodically monitor and evaluate compliance with this Code and its application to the Company's activities. The Board of Directors may amend this Code on the recommendation of the Governance Committee or of its own accord.

3. Information Management

3.1 Confidential Information

Information is a key asset for D-BOX. Our policy is to ensure adequate safeguards for confidential information exclusive to D-BOX, including confidential and exclusive information entrusted to D-BOX by third parties. All confidential information, including information on D-BOX's activities, assets, prospects, products, clients, suppliers and competitors, must be suitably protected against conscious or unconscious disclosure.
Relations between D-BOX, its team members and its clients are grounded in mutual trust and respect. To maintain this special relationship, we all have a responsibility to comply with D-BOX's policies and procedures, as well as the cultures and approaches of our clients.
As a full-fledge member of D-BOX, it is everyone's duty to protect the Company, to respect its clients, and to refrain from harming them. Each person targeted by the Code must behave in a courteous and civil manner.
Everyone is responsible for preserving the confidentiality and enhancing the quality of information.
The confidentiality of all information conveyed by the Company and sent by its clients and other third parties, including its suppliers, must be strictly maintained. Sharing information outside of work could adversely affect the Company's activities if that information is used against the Company by its competitors. Moreover, internal Company information that has not been publicly disclosed is potentially confidential information, and disclosure of this information outside of the Company, by spoken, written or electronic means, could have serious business, legal and regulatory consequences.
Confidential information must always be identified as such, may be disclosed only with the authorization of an officer and must be governed by an effective confidentiality agreement prior to disclosure. Everyone must also take appropriate steps to ensure that such confidential information is not disclosed internally, except to employees who require such information as part of their job at D-BOX. Each person must make every reasonable effort to protect the security and confidentiality of Company information.
For its part, D-BOX undertakes not to disclose, to anyone, any personal information about its employees, consultants, officers or directors, except with their prior consent, and not to intrude on their privacy.
Moreover, given that the relationship between the Company and its employees is based on trust, D-BOX will not intervene in their work unless it has reasons to doubt this relationship of trust.

When in doubt as to the use, conservation or dissemination of confidential information, by any means whatsoever, the legal department, human resources department or management must be consulted.

3.2 Privileged Information

Employees, consultants, officers and directors of the Company in possession of privileged information (important information not yet known to the public) are not permitted to reveal this information or to discuss it with anyone (including family and friends) except in the specific context of their work and with authorization

from an officer. Moreover, it is prohibited to conduct transactions involving Company securities before the information is made public.

3.3 Insider Trading

In addition to the executive officers and directors, certain employees may qualify as “insiders” because of their access to privileged information in the regular performance of their duties. Examples of privileged information include financial results, the development of a new product, a significant change in D-BOX’s objectives, a major discovery or a purchase or sale offer involving D-BOX.
Insiders are subject to very strict rules prohibiting them from trading D-BOX securities during certain periods. Insiders are also required to declare all transactions by set deadlines in order to avoid severe penalties from the Board of Directors and/or the President and CEO.

It is legally prohibited for any employee, officer or director of D-BOX who is in possession of privileged information to take part in transactions involving D-BOX securities (shares or options) until a reasonable period, i.e. at least two (2) full business days, has elapsed following the full disclosure of the privileged information in question, to allow wide dissemination of the privileged information.
Moreover, certain executives, officers and directors must report all transactions involving the Company’s securities on the site www.sedi.ca within five (5) calendar days of the transaction date.
Breaking these rules may result in severe penalties for the insider, who is solely responsible for complying with the rules prohibiting trading.
For additional information on this topic, the *Policy on Insider Trading* is available upon request. Employees can also speak to their manager about this.

3.4 Intellectual and Physical Property

D-BOX is the sole owner of the copyright on the works created by its employees in the course of their employment with the Company. For example, without limitation, computer programs, studies, presentations, manuals and other documents produced as part of their work are and remain the Company’s property.

Each employee, consultant and officer must undertake, once hired, to surrender all other intellectual property rights, titles and interests, of any nature whatsoever, in anything that may have been or could be produced, designed and/or performed by the employee, alone or with others, as part of or during his term with D-BOX, as and when they are created. As such, all employees are given an assignment of rights agreement pertaining to the following:

- rights, titles and interests as the inventor, and in any invention patents to be filed, pending, or registered;
- rights, titles and interests in one or more trademarks;
- rights, titles and interests in any industrial design.

This agreement also states that each D-BOX employee waives any moral right to the foregoing in favour of the Company, for all purposes and for the entire duration of said moral right. It also includes an undertaking to sign any document required to give full effect to said assignment and **to cooperate fully in the application for, acquisition and registration, by D-BOX, of any intellectual property right** covering the foregoing in Canada, the United States of America or elsewhere in the world.

D-BOX also undertakes to respect the intellectual property rights of third parties. Each employee, consultant, officer and director of the Company must take reasonable measures to ensure that their actions, as part of their activities within the Company, do not violate the rights of third parties (copyrights, invention patents, industrial designs, trademarks). The Legal Department can be consulted when in doubt as to the use of material from a third party or the need to obtain a third party's prior authorization to use an item potentially covered by one or more intellectual property rights.
The Company provides everyone with the equipment needed to do their work efficiently. These tools and related usage rights are the exclusive property of D-BOX. It is everyone's responsibility to ensure that they are not damaged and are returned in their original condition when no longer needed.

4. Conflicts of Interest

4.1 Conflicts of Interest

The Board of Directors has adopted the following rules to make it easier to determine whether a relationship or a transaction constitutes a conflict of interest. The Board of Directors has determined that the following pose an inappropriate conflict of interest under this Code. This list is not exhaustive and is subject to review and revision from time to time by the Board of Directors.

Personal interests and relationships must not adversely affect the interests of the Company. Any real or apparent conflict of interest between personal interests and those of the Company must be handled objectively and in accordance with the following procedures. Any conflict of interest is forbidden unless it has gone through the process of disclosure, consultation and approval described below.

A conflict of interest arises when a person favours his own interests or those of his friends and family members over the interests of D-BOX and its clients. Each person to whom this Code applies must ensure, in his work and personal activities, to always act in D-BOX's best interest. Actual or apparent situations of conflict of interest with D-BOX must be avoided at all times and it is everyone's duty to remain loyal to the Company. A conflict of interest may affect the Company directly or place it in a conflictual situation.
It should also be noted that the restrictions on conflicts of interest and on accepting prohibited benefits also apply to family members, dependents and related individuals. Everyone should be aware of their liability for any conflict that may arise as a result of their conduct or the consequences of any prohibited benefit they may receive.

4.2 Prohibited Actions

An employee, consultant or officer must not:

- serve as an employee, officer, director, advisor, consultant (directly or through an organization) or in any other capacity for a client, a supplier or a direct competitor of the Company, except on request from and/or with the prior approval of the President and CEO and the CFO;
- have a financial interest in a supplier or a client of the Company, other than a direct investment constituting less than five percent (5%) of the voting rights in a public company or less than five percent (5%) of the voting rights in a private corporation; or
- have a financial interest in a direct competitor of the Company.

Here are some other examples of conflictual situations that must be avoided:

- Taking a second job:

- with a supplier or a client, without the prior authorization of Human Resources and the President and CEO;
- with a competitor;
- that prevents the person from performing to his full capacity in his work at D-BOX;
- that could tarnish the image of D-BOX.

- Subsidizing, sponsoring or becoming involved in political, religious or other organizations **on behalf of D-BOX**, without having obtained prior authorization;

- For an employee or an officer, direct supervision of an employee who is a family member or a close relative, e.g. spouse, parent, brother or sister, child, mother-in-law or father-in-law, son-in-law or daughter-in-law, brother-in-law or sister-in-law, as well as any family member living at the same address as the employee or officer;

- Offering a gift, favour or incentive to a client, supplier or competitor equivalent to or worth more than one hundred fifty dollars ($150) and with the intention of benefiting personally;

- Receiving a gift, favour or incentive from a client, supplier or competitor equivalent to or worth more than one hundred fifty dollars ($150) (see the policy on gifts and favours below);

- Soliciting gifts or favours.

An officer or senior executive of the Company must not:

- render significant services as an employee, officer, director, advisor, consultant (directly or through an organization) for other companies or organizations without disclosing said services and obtaining the prior approval of the Company. Generally, this requires disclosure to and approval of the Chair of the Governance Committee.

A director who is not employed by the Company must not:

- serve as an employee, officer, director, advisor, consultant (directly or through an organization) or in any other capacity for a direct competitor of the Company;

- have, or allow any close relative to have, a financial interest in a direct competitor of the Company;

- use his position with the Company to influence any decision by the Company concerning a contract or a transaction with a supplier or a client of the Company:
    - if he, or a close relative of his, renders services as an employee, officer, director, advisor, consultant (directly or through an organization) or in any other capacity for such a supplier or client; or has a financial interest in such a supplier or client; or incites, assists or otherwise participates, directly or indirectly, in the involvement of a close relative with a major supplier, a major client or a direct competitor of the Company in a manner that would be prohibited for an employee or an officer, in any of the prohibited activities listed above. Note that the term “close relative” of a person includes his spouse, parents, brothers and sisters, children, in-laws, sons-in-law or daughters-in-law, brothers-in-law or sisters-in-law, and any relative living at the same address.

Moreover, any director, executive officer or person holding, directly or indirectly, more than 10% of the voting rights in the Company, and related persons or people belonging to the same group as the latter, must disclose their interest, direct or indirect, by indicating

its approximate value, in any transaction concluded in the last three (3) fiscal years or in the current year, which had or which one can reasonably assume will have a significant impact on the Company. When in doubt, it is recommended to contact the Legal Department.

Every person to whom this Code applies must disclose any actual or reasonably apparent conflict of interest, including any current or proposed transaction, or any relationship that could reasonably give rise to a conflict of interest. An employee or a consultant must disclose this information to his immediate supervisor (or, if that person is involved in the matter, to the Company's Legal Department), who is responsible for discussing it with the President and CEO or the Chair of the Governance Committee, as applicable. Officers and directors must speak to the President and CEO or the Chair of the Governance Committee.

4.3 Procedures for Determining Conflicts of Interest and Exemptions

In determining whether a conflict of interest exists and whether an exemption from a rule of the Code is needed in a particular situation, the President and CEO or, where applicable, the Chair of the Governance Committee and the Board of Directors, as the case may be, should also consider:

- **The person involved in the potential conflict** – For example:
  - Whether the person is an officer or director of the Company and, in the case of a director, whether he is an independent director.

- **The nature of the relationship or situation creating the potential conflict of interest** – For example:
  - Does the controversy arise from the fact that the person is an officer or director of a party doing business with the Company?
  - Is the director or officer of the Company related to a person who is an officer or director of the party doing business with the Company?

  The more distant the person's relationship with any one of the companies involved, the lower the risk that this person may be capable of influencing the Company's current decisions and, consequently, that the relationship or activity may be detrimental to the Company;

- **The nature of the entity to which the director or officer is related** – For example:
  - Is this entity a competitor of the Company, a collaborator, a supplier or a client, and what is its importance to the Company?

- **The nature of the proposed transaction**, including:
  - the importance of the transaction;
  - whether the Company has previously engaged in this type of transaction, with this party or others;
  - the other relationships with the other party;
  - the leverage of the other party;
  - whether there were unusual terms associated with the transaction;
  - whether the terms offered are those that the Board of Directors would offer or could obtain if the relationship did not exist;

- the degree to which the officer or director raising the concerns is involved in any of the proposed transactions, including whether the person requesting the exemption receives remuneration or any other benefit as a result of the transaction;
  - whether the person took advantage of a business opportunity;
  - whether the proposed transaction or relationship would result in a director losing his independent status; and
  - how disclosure of the situation would be perceived in, for instance, the newspapers or some other public forum.

After examining these considerations and all other matters deemed relevant, the officer or the Chair of the Governance Committee, as the case may be, should then consider whether the relationship or activity: (i) will adversely affect the Company; (ii) was undertaken in good faith; (iii) constitutes disloyalty to the Company and its shareholders; (iv) constitutes a breach of the laws governing the Company; and (v) confers an undue personal advantage on the person. The officer or the Chair of the Governance Committee should then be in a position to determine whether a conflict of interest exists and, if so, whether this conflict is acceptable to the Company under the circumstances.

The following questions may also be useful:

- Is it legal?
- Is it fair?
- Would I be comfortable with other people knowing what I did?
- How would I feel if this was covered in the newspapers?
- What would I tell my child or a close friend to do in a similar situation?

5. Gifts, Favours and Corruption

All employees, officers and directors must conduct their business in such a way as to avoid adversely affecting their judgment or the reputation of the Company. In general, all persons must refuse, and not offer, advantages that target one person in particular, unless the advantage in question has a symbolic value, is not in cash and does not affect the Company's image or the public's perception.

5.1 Gifts and Favours

Any person who receives a gift, favour or incentive worth more than $150 that could affect his independence or objectivity now or in the future, must refuse it and declare it to management. Any exception to this rule must be fully justified and approved in advance by the President and CEO for employees and by the Governance Committee for the President and CEO and other executive officers.

5.2 Corruption

Corruption is a criminal act. No person in the Company may offer or give any form of bribe or kickback to any government representative or any other person, organization or company to ensure preferential treatment in connection with the Company's affairs. Modest, conventional entertainment or promotional items that comply with Company parameters and are not intended to ensure preferential treatment are generally acceptable.

All officers, directors, employees, agents and shareholders acting on behalf of the Company must comply with the anti-corruption, accounting and recording provisions of the *Corruption of Foreign Public Officials Act.* This act prohibits the Company and any person acting on its behalf from giving, offering or promising, directly or indirectly, a monetary payment or other item of value to a foreign representative or a foreign political party with the aim of influencing that representative in any way to assist the Company in securing or retaining business. The civil and criminal penalties this law imposes on offending individuals and businesses are severe. If there is a doubt about whether a payment or a gift would violate this act, the matter must be referred to the Legal Department before any action is taken.

6. Operations Management

6.1 Fair Operations

Every employee, officer, consultant or director must strive to deal honestly, morally and fairly with suppliers, clients, competitors and employees of the Company. Statements regarding Company products and services should not be false or ambiguous. It is prohibited to take unfair advantage of any person by manipulating, concealing or abusing privileged information, misrepresenting important elements or engaging in any other unfair practice.

6.2 Protection of Company Assets and Opportunities

The entire staff should seek to protect the Company's assets. It is prohibited for a person to take personal advantage of opportunities discovered through his position in the Company. All transactions conducted on behalf of the Company and all uses of the funds, facilities and other assets of the Company must be limited to the framework of the Company's business, comply with the authorization granted and be properly documented.

6.3 Accuracy of Books, Files and Reports

All of the Company's books, files and accounts shall be kept in compliance with all applicable regulations and standards, and shall accurately reflect the true nature of the recorded transactions. Each person is responsible for the accuracy of his files and reports. No undisclosed or unrecorded accounts or reserves shall be set up for any purpose whatsoever.

6.4 Procedures for Accounting-related Complaints to the Governance Committee

The Governance Committee has established the following procedures for the receipt, retention and processing of complaints and concerns regarding accounting, internal accounting controls and financial auditing matters.

Complaints and concerns related to accounting may be reported to the Company's President and CEO or Chief Financial Officer, or may be submitted confidentially to the Chair of the Governance Committee.

All complaints and concerns reported with regard to accounting must be transferred to the Chair of the Governance Committee. They will be analyzed and resolved under the supervision of the Governance Committee by persons the Governance Committee deems appropriate. Confidentiality will be maintained to the greatest possible extent in keeping with the need to conduct a proper investigation.

The Company may not punish, discriminate or retaliate against any person who may report such conduct in good faith, whether or not the information is ultimately proven, or who cooperates in any investigation or inquiry into such conduct.

A record of all accounting-related complaints and concerns, tracing their reception, investigation and resolution, shall be kept by the Governance Committee. Copies of written complaints and concerns, and records thereof, shall be kept in accordance with the Company's policy on document retention and shall be available for examination by the Company's external auditor.

7. Policy on Whistleblowing and Protection

7.1 Purpose of the Policy

The purpose of this policy is to encourage Company employees to report acts of wrongdoing, assuming employees will act in good faith and will not bring false accusations. An employee who knowingly or recklessly makes declarations or reports that are not in good faith is liable to disciplinary action, up to and including dismissal. Employees who report acts of wrongdoing under this policy are and will continue to be subject to the general performance standards governing Company employees. Consequently, an employee who reports acts of wrongdoing under this policy against whom legitimate adverse action has been taken or is considered, such as poor work performance or misconduct but excluding prohibited retaliation, may not use this policy as a defence against the legal action taken by the Company.

7.2 Object

This policy confirms the Company's ongoing commitment to the integrity and ethical conduct of its employees. It establishes the procedures through which Company employees may submit concerns about any suspicious conduct, including but not limited to accounting irregularities, acts of fraud, corruption, or any other violations of internal policies and applicable laws, to the Chair of the Audit Committee of the Board of Directors, without fear of retaliation.

7.3 Protection Measures

The Company must not take adverse action against an employee in retaliation for:

- accusations of acts of wrongdoing brought in good faith in accordance with this policy;
- information provided, or acts that result in information being provided, in an investigation conducted by an organization or a regulatory authority or a person in the Company who has a supervisory or similar power over the employee, concerning any conduct which the employee believes in good faith to constitute a breach of applicable laws, regulations or rules governing securities or any statutory provision concerning a fraud whose victims are Company shareholders; or
- participation in an inquiry, hearing, legal proceeding or administrative investigation conducted in the context of a report of acts of wrongdoing.

7.4 Procedures

7.4.1 Disclosure

We urge employees with concerns related to any unethical or any suspicious conduct to report these situations promptly to the Chair of the Compensation and Corporate Governance Committee, by e-mail or letter. Here is the contact information of the current Chair of the Compensation and Corporate Governance Committee:

Chair of the Compensation and Corporate Governance Committee
Contact details for the Chair of the Compensation and Corporation Governance Committee are available on the Company's website at the following address:
https://www.d-box.com/en/investors/leadership-and-governance

7.4.2 Timing

The earlier a concern is expressed, the easier it is to take corrective action.

7.4.3 Evidence

While the employee is not expected to prove the truth of an allegation, he must demonstrate that there is sufficient cause for concern.

7.4.4 Confidentiality

To the extent possible, the identity of the employee who has made a disclosure under this policy will not be revealed to persons in his department, division or workplace. The Company will make genuine efforts to protect the confidentiality of employees who make disclosures; it being understood, however, that the Company or its employees and agents are entitled to reveal the identity of the employee who made the disclosure and the confidential information concerning him to the extent necessary to allow for an effective, in-depth investigation.

7.5 Processing of Complaints

The action taken will depend on the nature of the issue. The Governance Committee of the Board of Directors of the Company will receive a report for each complaint filed, and the steps taken to address the complaint will be followed up on.

7.5.1 Report to the complainant

Within 30 days of receipt of the complaint, the Company will give the complainant notice:

- acknowledging receipt of the complaint;
- indicating how the complaint will be dealt with; and
- estimating the time required to obtain a final response.

7.5.2 Other information

Depending on the nature of the complaint and the clarity of the information provided, the Company may seek to obtain further information from the complainant. Subject to legal constraints, the complainant will be kept informed of the outcome of the investigations.

7.6 Complaints about Retaliatory Action

Complaints about retaliatory action should be submitted by e-mail or letter to the Chair of the Governance Committee of the Board of Directors of the Company. See the resource person's contact information in 7.4.1, above.

8. Special Obligations of the President and CEO and Senior Officers

The Company's policy is to make a full, correct, precise, timely and comprehensible disclosure in accordance with all applicable laws, codes and regulations, in all of the reports and documents the Company publishes or submits to the regulatory authorities and in all of the Company's other public communications.

The President and CEO of the Company, as well as the Chief Financial Officer, the senior vice-presidents and persons acting in a similar capacity (collectively referred to as "senior officers") are each required to comply with this policy and to promote adherence to this policy by all employees. Individually, the President and CEO and senior officers also have the following specific responsibilities:

- Ensuring that the Company maintains: (i) adequate control of its assets and financial communications; and (ii) suitable procedures and controls to ensure a full, correct, precise, timely and comprehensible disclosure in all reports and documents that the Company publishes or submits to the regulatory authorities, and in all of the Company's other public communications;
- Demonstrating leadership in the establishment of a culture of high moral principles and commitment to maintaining compliance, fostering a work climate that encourages employees to express their concerns, responding promptly to those concerns, and acting honestly and morally;
- Promptly bringing to the attention of the Company's Governance Committee any important information of which he may have knowledge and which affects the Company's disclosures in its public communications and statements.
- Promptly bringing to the attention of the Company's Governance Committee any important information he may have concerning: (i) significant defects in the design or operation of internal controls that could adversely affect the Company's ability to record, process, summarize and announce financial data; and (ii) any fraud, significant or not, involving management or other employees having key roles in the Company's financial reports, disclosures and internal controls.
- Promptly bringing to the attention of the Chair of the Governance Committee any important information he may have concerning any breach of this Code by any member of management or by any other employee having a key role in the Company's financial reports, disclosures and internal controls.
- Promptly bringing to the attention of the Company's Legal Department and to the Chair of the Governance Committee any important information he may have concerning evidence of a significant breach, by the Company or by any one of its agents, of securities or other laws, or of the codes and regulations applicable to the Company and its operation.

9. Appendix – Security procedure for economic intelligence

9.1 General principle

D-BOX's most important competitive advantage lies in its knowledge and know-how. In fact, intellectual property and data related to its technological, industrial and innovative processes have made D-BOX the thriving company it is today. This being said, D-BOX is not impervious to potential competitors who may see in this advantage a business opportunity and attempt to steal or use economic or sensitive Company information, which could jeopardize its financial soundness. D-BOX has therefore implemented standards to ensure the authentication, classification control and protection of economic intelligence.

Each employee has the duty to comply with effective practices and policies adopted with respect to security, and to employ any means necessary to treat sensitive information in an appropriate manner.

* Please note this procedure is applied in conjunction with the **policies set out in section 5 of the Employee Guide.**

9.2 Definitions

9.2.1 Espionage

Espionage is defined as illegal, clandestine, coercive or deceptive activity engaged in or facilitated by a private or public company and designed to gain unauthorized access to economic intelligence, such as proprietary information or technology, for economic advantage.[1]

9.2.2 Economic intelligence

Economic intelligence is policy or commercially relevant economic information, including technological data, financial, proprietary commercial and government information, the acquisition of which by foreign interests could, either directly or indirectly, assist the relative productivity or competitive position of the economy of the collecting organization's country.[2]

At D-BOX, economic intelligence includes but is not limited to the following:

- ✓ Client and supplier data;
- ✓ Ongoing development and innovation projects;
- ✓ Manufacturing methods and procedures;
- ✓ Motion Code and the databases;
- ✓ Organizational or financial Information that could influence the share price;
- ✓ Ongoing movie projects;
- ✓ Etc.

9.3 Procedure

The information in this section is taken, in its entirety, from the website of the Canadian Security Intelligence Service. The entire text can be found at https://www.csis.gc.ca/prrts/spng/mthds-eng.asp.

9.3.1 Risk situations and preventive approach

Several well-known modus operandi (MO) are used by foreign governments attempting to acquire sensitive corporate or proprietary information. These include:

9.3.1.1 Unsolicited requests for proprietary information

Unsolicited requests for proprietary or classified information are associated with foreign collection activity. Requests frequently involve faxing, mailing, e-mailing, or phoning individuals rather than corporate marketing departments. The requests may involve surveys or questionnaires and are frequently sent over the Internet.

Marketing surveys can elicit sensitive technological and business information. With this particular method it is important to consider who is the end-user of the information and who is completing the survey. Increasing use of the Internet provides a method of direct communication with government and American industry for foreign collection purposes.

How to spot a potential risk related to a request for information

- The Internet address is in a foreign country.
- The recipient has never met the sender.
- Information on the technology requested is classified, export-controlled, or has both commercial and military applications.
- The requester identifies his/her status as a student or consultant.
- The requester identifies his/her employer as a foreign government or the work is being done for a foreign government or program.
- The requester asks about a defence-related program, project, or contract.

- The requester asks questions about defence-related programs using acronyms specific to the program.
- The requester admits he or she could not get the information elsewhere because it was classified or controlled.
- The requester advises the recipient to disregard the request if it causes a security problem or if it is for information the recipient cannot provide due to security classification, export controls, and so forth.
- The requester advises the recipient not to worry about security concerns.
- The requester assures the recipient that export licenses are not required or are not a problem.
- Marketing surveys may be faxed or mailed to an individual via the company marketing office.
- Marketing surveys may be sent by foreign consortiums or consulting companies. Foreign companies with foreign intelligence involvement are likely to be a consortium of officials, military officers, or private interests.
- Marketing surveys often may exceed generally accepted terms of marketing information.
- Strong suspicions that the "surveyor" is employed by a competing foreign company.
- Surveys may solicit proprietary information concerning corporate affiliations, market projections, pricing policies, program or technology director's names, company personnel working on the program, purchasing practices, and types and dollar amounts of American government contracts.
- Customer and supplier bases for a company may also be sent marketing surveys that exceed accepted terms of marketing information.

9.3.1.2 Inappropriate conduct during visits

Foreign visits to American companies can present potential security risks if sound risk management is not practised and appropriate security measures implemented.

How to spot a potential risk related to a visit

- Visitors are escorted by a diplomatic or embassy official who attempts to conceal their official identities during a supposedly commercial visit.
- Hidden agendas, as opposed to the stated purpose of the visit; that is, visitors arrive to discuss program X but do everything to discuss and meet with personnel who work with program Y.
- Last minute and unannounced persons added to the visiting party.
- "Wandering" visitors, who act offended when confronted.
- Using alternate mechanisms. For example, if a classified visit request is not approved, the foreign entity may attempt a commercial visit.
- Visitors ask questions outside the scope of the approved visit, hoping to get a courteous or spontaneous response.

9.3.1.3 Suspicious work offers

Foreign scientists and engineers will offer their services to research facilities, academic institutions, and defence contractors. This may be an MO to place a foreign national inside the facility to collect information on a desired technology.

How to spot a potential risk related to a suspicious work offer

- Foreign applicant has a scientific background in a specialty for which his country has been identified as having a collection requirement.
- Foreign applicant offers services for free. Foreign government or corporation associated with government is paying expenses.
- Foreign interns (students working on Masters or Doctorate degrees) offer to work under a knowledgeable individual for free, usually for a period of two to three years.
- The information on the technology the foreign individual wants to research is proprietary, classified, or export-controlled.

9.3.1.4 Targeting at international exhibits, seminars, and conventions

International exhibits, seminars and conventions offer opportunities to link programs and technologies with knowledgeable personnel but such events can also present some security risks.

How to spot a potential risk related to targeting

- Topics at seminars and conventions deal with classified or controlled technologies and/or applications.
- The country or organization sponsoring the seminar or conference has tried unsuccessfully to visit the facility.
- Invitation to brief or lecture in a foreign country with all expenses paid.
- Requests for presentation summary 6-12 months prior to seminar.
- Photography and filming appear suspicious.
- Attendees wear false or incomplete name tags.

9.3.1.5 Exploitation of joint ventures and joint research

Co-production and various exchange agreements potentially offer significant collection opportunities for foreign interests to target restricted or proprietary technology.

How to spot a potential risk related to joint research

- Foreign representative wants to access the local area network (LAN).
- Foreign representative wants unrestricted access to the facility.
- Enticing American contractors to provide large amounts of technical data as part of the bidding process, only to have the contract cancelled.
- Potential technology-sharing agreements during the joint venture are one-sided.

- The foreign organization sends more foreign representatives than are necessary for the project.
- The foreign representatives single out company personnel to elicit information outside the scope of the project.

9.3.1.6 Acquisitions of technology and companies

Foreign entities attempt to gain access to sensitive technologies by purchasing American companies and technologies.

How to spot a potential risk related to a suspicious purchase offer

- New employees hired from the foreign partner's company, or its foreign partners, wish to immediately access sensitive corporate or proprietary information.

9.3.1.7 Co-opting of former employees

Former employees who had access to sensitive, proprietary, or classified program information remain a potential counter-intelligence concern. Targeting cultural commonalities to establish rapport is often associated with the collection attempt. Former employees may be viewed as excellent prospects for collection operations and considered less likely to feel obligated to comply with American export controls or company security requirements.

How to spot a potential risk related to false solicitation

- Former employee took a job with a foreign company working on the same technology.
- Former employee maintains contact with former company and employees.
- Employee alternates working with American companies and foreign companies every few years.

9.3.1.8 Targeting cultural commonalities

Foreign entities exploit the cultural background of company personnel in order to elicit information.

How to spot a potential risk related to cultural targeting

- Employees receive unsolicited greetings or other correspondence from embassy of country of origin.
- Employees receive invitations to visit country of family origin for the purpose of providing lecture or receiving an award.
- Company personnel are singled out by foreign visitors of same cultural background to socialize.

9.4 Security rules

9.4.1 When a potential rusk is identified

Employees who are faced with a situation described above and have even the slightest doubt about the source, intention or actions of another party must do the following:

a. Systematically stop all activities and interactions with the other party.
b. Immediately stop using computer systems or other means of communication.
c. Immediately inform:
   - their immediate supervisor or another executive officer who is there;
   - Information Technologies management; and
   - Human Resources management.

Employees who signal a potential risk in good faith will face no consequences, unless their intention is clearly to cause harm to someone or a statement is proven to be false. If such is the case, disciplinary measures may be imposed, up to and including dismissal.

9.4.2 Preventive security measures

To ensure the Company's sensitive and/or confidential economic intelligence is managed securely, we ask employees to apply the following security measures, especially while travelling:

i. Store data and documents containing sensitive information under lock and key, or keep them with you while travelling.

ii. Properly dispose of documents containing sensitive company information.

iii. Protect access codes and passwords; employees are responsible for all forms of communication requiring their access codes or passwords.

iv. Do not use the same password for professional activities at D-BOX and for personal reasons (e.g. home Internet service provider account, online business site, public e-mail server).

v. Only discuss sensitive company business in secure locations: be careful in common areas, restaurants and public transit, where such conversations are to be kept to a minimum.

vi. When working on a portable computer in a public area, be sure the information on the screen is not visible to someone behind or above you.

vii. Apply the following principle to all sensitive data: does this person absolutely need to know this information?

viii. Be careful and judicious when choosing a means of communication for business discussions (for example, cell phones, faxes and telephone lines).

ix. When using a storage device from which information cannot be deleted because it is read-only (CD, DVD, etc.), be sure to make the information unreadable before disposal.

x. Never deactivate an antivirus program, a password system or any other data protection system (e.g. physical lock, biometrics) which has been installed and deemed secure by Information Technologies.

xi. Never leave a portable computer, cell phone or other communication or storage device where another person or entity could access it. A hotel room is not considered to be a secure location, as it can easily be accessed by many people.

xii. Protect all external data storage systems (hard drives, USB flash drives) with a secure password.

xiii. There are strict limitations for using the D-BOX wireless network. It may only be accessed for professional purposes by members of the Board of Directors or people duly authorized to do so. No other person should be granted access to this network for any reason whatsoever. Information Technologies uses every means to detect and disable any wireless device that is unauthorized.