identitii

Identitii Limited
ACN 603 107 044
ASX:ID8

People & Culture Policy

Introduction

Context

The People & Culture Policy is developed to provide a framework for managing the organisation's people operations in a fair, inclusive, and consistent manner. It recognises the importance of fostering a positive work environment, attracting and retaining talented employees, and promoting their development and well-being. The policy takes into account relevant legal requirements, industry best practices, and the organisation's values and goals.

Purpose

The purpose of the People & Culture Policy is to establish guidelines, procedures, and principles for managing various aspects related to employees throughout their employment lifecycle. It aims to create a supportive and inclusive culture that values diversity, promotes fairness, and respects the rights and well-being of individuals. The policy serves as a reference for both employees and management to ensure consistent and equitable treatment in all people-related matters.

Scope

The People & Culture Policy applies to all employees of the organisation, including full-time, part-time, temporary, and contract workers, regardless of their level or role. It encompasses various areas, such as recruitment and selection, onboarding, offboarding, role changes, remote and flexible work arrangements, social media use, competence development, worker rights and responsibilities, recruitment referral programs, diversity initiatives, family and domestic violence leave, and health and well-being support. The policy and its associated standards are applicable across all departments and locations of the organisation.

Objectives

1. Fair and Inclusive Work Environment:
    a. The policy aims to foster a work environment that is free from discrimination, harassment, and bias.
    b. It promotes fairness and equal opportunities for all employees, regardless of their background, gender, age, race, ethnicity, sexual orientation, or disability.
2. Effective Recruitment and Selection:
    a. The policy provides guidelines for attracting and selecting qualified candidates through transparent and unbiased processes.
    b. It seeks to ensure that recruitment efforts align with the organisation's goals and values while embracing diversity.
3. Seamless Onboarding and Offboarding:
    a. The policy outlines procedures for efficiently integrating new employees into the organisation and ensuring a positive experience.
    b. Similarly, it establishes guidelines for managing the departure of employees in a respectful and professional manner, while protecting the organisation's interests.

4. Flexible Work Arrangements:
    a. The policy supports remote and flexible work arrangements where applicable, allowing employees to achieve a work-life balance and maintain productivity.
    b. It provides guidelines for establishing expectations, communication, and performance measurement in these work arrangements.
5. Continuous Competence Development:
    a. The policy emphasises the organisation's commitment to supporting employees' professional growth and development.
    b. It promotes access to training, learning opportunities, and career advancement programs to enhance employees' skills and capabilities.
6. Worker Rights and Responsibilities:
    a. The policy clarifies the rights and responsibilities of employees within the organisation, ensuring that they are treated fairly, provided a safe working environment, and aware of their obligations regarding performance, conduct, and compliance with policies.
7. Diversity and Inclusion:
    a. The policy recognises the value of diversity and aims to foster an inclusive workplace where all employees feel respected, valued, and empowered.
    b. It seeks to implement initiatives that promote diversity, equity, and inclusion, while addressing any barriers or biases that may exist.
8. Employee Health and Well-being:
    a. The policy highlights the organisation's commitment to promoting employee health and well-being.
    b. It provides access to resources, programs, and support mechanisms that prioritise physical, mental, and emotional well-being.

By establishing these objectives, the People & Culture Policy aims to create a positive work environment that attracts and retains talented individuals, supports their growth, and upholds ethical and inclusive practices throughout the organisation.

Mandatory policy statements

Requirements applicable to all staff

1. Code of Conduct:
    a. All staff members are expected to adhere to a code of conduct that outlines expected behaviours, ethics, and standards of professionalism.
2. Compliance with Policies and Procedures:
    a. Employees are required to comply with all organisational policies, procedures, and guidelines applicable to their roles.
3. Confidentiality and Data Protection:
    a. Staff members may be required to maintain confidentiality of sensitive information and comply with data protection regulations.
4. Health and Safety:
    a. Employees must follow health and safety protocols, report any hazards or incidents promptly, and contribute to maintaining a safe work environment.
5. Professionalism and Respectful Behaviour:
    a. All staff members should exhibit professionalism and treat colleagues, clients, and stakeholders with respect, regardless of their position or background.

6. Attendance and Punctuality:
    a. Employees are expected to be punctual, follow attendance policies, and inform their supervisors or P&C in case of planned or unplanned absences.
7. Performance and Productivity:
    a. Staff members are required to perform their job duties to the best of their abilities, meet performance expectations, and contribute to achieving organisational goals.
8. Continuous Learning and Development:
    a. Employees may be expected to participate in training programs, skill development activities, and professional growth opportunities to enhance their knowledge and capabilities.
9. Reporting of Issues and Concerns:
    a. All staff members should report any violations of policies, unethical behaviour, or concerns related to workplace issues through appropriate channels.
10. Use of Company Resources:
    a. Employees must use company resources, such as equipment, facilities, and technology, responsibly and for authorised purposes.
11. Conflict of Interest:
    a. Staff members may be required to disclose any potential or actual conflicts of interest and act in the best interests of the organisation.
12. Staff Screening:
    a. All Staff may be subject to background screening checks.
    b. The level of checks to be performed commensurate with the role type.
    c. Any discrepancies identified, or unable-to-verify checks must be assessed, assured by compensating controls and endorsed by relevant stakeholders before clearance for appointment.

Requirements applicable to line managers

1. Leadership and team management:
    a. Line managers are expected to provide effective leadership, guidance, and support to their teams, fostering a positive work environment and promoting collaboration and teamwork.
2. Performance management:
    a. Line managers are responsible for setting performance expectations, conducting regular performance evaluations, providing feedback and coaching, and addressing any performance issues or concerns within their teams.
3. Workforce planning and resource allocation:
    a. Line managers may be involved in workforce planning activities, including assessing staffing needs, participating in recruitment and selection processes, and allocating resources effectively within their teams.
4. Training and development:
    a. Line managers are responsible for identifying training and development needs within their teams and facilitating opportunities for their team members' skill enhancement and professional growth.
5. Conflict resolution:
    a. Line managers are expected to handle conflicts and disputes within their teams effectively, promoting open communication, addressing concerns, and mediating conflicts when necessary.

6. Communication and feedback:
    a. Line managers should maintain regular and effective communication with their team members, providing clear expectations, sharing relevant information, and offering constructive feedback.
7. Employee engagement:
    a. Line managers play a crucial role in fostering employee engagement and motivation within their teams, promoting a positive work culture, recognizing achievements, and addressing any concerns or issues that may impact morale.
8. Leave and absence management:
    a. Line managers may be responsible for approving and managing employee leave requests, ensuring appropriate coverage and workload distribution within their teams.
9. Policy and procedure implementation:
    a. Line managers are responsible for ensuring their teams' compliance with organisational policies, procedures, and guidelines, including health and safety regulations, performance management processes, and other relevant policies.
10. Succession planning and talent development:
    a. Line managers may be involved in identifying and developing potential successors within their teams, ensuring continuity and effective talent management within the organisation.

Code of conduct

Our values and commitments

The Company's core values and commitments are:

1. One team:
    a. We are all in this together and are driving towards the same goals.
    b. We are team players and look out for each other.
2. People first:
    a. A happy home life makes us stronger.
    b. Sometimes what's right for the business is prioritising ourselves and our families.
3. Leverage genius:
    a. Teach and share knowledge.
    b. Be curious and use insights.
    c. Ask for help to solve problems.
4. Be real:
    a. Ask for what you need to be your best.
    b. Help others be their best.
    c. When you're not at your best, embrace it.
5. Finish it:
    a. Don't let a good thing go undone.
    b. Plan to finish what you start, one way or another.
    c. Ask for help to finish something, share the win.

Our ethical standards

Conflicts of interest

A conflict of interest exists where loyalties are divided. For example if you or your relatives or associates have a personal or commercial interest which may interfere, or be perceived to interfere, with the performance of your duties and responsibilities to the Company, making it difficult to perform your role objectively and effectively. It is imperative that you are able to manage a conflict of interest when it arises.

You must act in the best interests of the Company. To safeguard the confidence of the Company's key stakeholders in the Company's integrity, it is paramount that you do not allow personal interests or the interests of relatives or associates to conflict with the interests of the Company. You must avoid participating in decisions and activities which may conflict, or be perceived to conflict, with your duties and responsibilities to the Company.

Financial interests in other businesses and outside memberships

You must not enter into any arrangement or participate in any activity that would conflict with the Company's best interests or would be likely to negatively affect the Company's reputation.

You must not be involved in any other company or business or organisation as director, agent, employee or consultant, whether paid or unpaid, if there is a possibility that your personal interests could conflict, or be perceived to conflict, with those of the Company unless you obtain approval first from the Company Secretary or the Board (if you are a director).

If you are involved in a conflict or possible conflict, or become aware of a conflict, you must tell the Company Secretary or the Board (if you are a director) as soon as possible.

Corporate opportunities, benefits and ownership of work

You must not use Company or customer property, or information, your position or opportunities which arise from these to improperly gain benefit for yourself or for another party or to cause detriment to the Company or its customers.

You have an obligation to avoid all financial, business and other arrangements which may be opposed to the interests of the Company, or which may place you in a competitive position with the Company.

The product of any work performed while you are with the Company, or on behalf of the Company, or using Company property (including all intellectual property rights created in connection with that work) belongs to the Company.

Anti-bribery and gifts

A number of countries, including Australia, have strict laws against bribery and corruption. The anti- bribery laws of some countries including Australia and the United States can apply to things done in other countries (i.e. wide-reaching extra-territorial effect). We must comply with and uphold all laws against bribery, corruption and related conduct applying to the Company in all the jurisdictions where the Company operates.
Accordingly, the Company has a strict policy not to offer secret commissions or bribes to further its business interests. Depending on the circumstances, facilitation payments may breach anti-bribery laws.

Naturally, you must not accept any money or opportunity or other benefit which could be interpreted as an inducement, secret commission or bribe. Care must be exercised in accepting hospitality, entertainment or gifts over and above that required for the normal conduct of business or which may compromise your impartiality.

We are committed to adopting effective systems to counter bribery and related improper conduct and to monitoring and enforcing these systems. From time to time, we may issue further guidance regarding what is acceptable in the normal course, what you can do with Board approval and what is prohibited.

You may also seek further information or clarification from the Company Secretary, legal counsel, the Board (if you are a director) or other relevant advisor.

See the Anti-Bribery and Anti-Corruption Policy for more information.

Politicians, government officials and lobbying

All dealings with politicians and government officials which relate to the Company and its business activities must be conducted at arm's length and with the utmost professionalism, to avoid any perception of attempts to gain advantage or to improperly influence the outcome of an official decision.

You must not make any donation or other financial contribution to any political party or candidate for an election or sponsor any organisations (other than in a purely personal capacity) without seeking and obtaining prior approval from the Company Secretary. Under this Code, all payments to government officials to secure an advantage, including payments to expedite or secure the performance of routine action, are prohibited.

Without specific authorisation from the Company, you must not engage in any lobbying of political officials, elected or appointed. Lobbying activity generally includes the attempt to persuade such officials to follow a particular course of action or policy or attempts to influence the passage or defeat of legislation and may trigger registration and reporting requirements. In many jurisdictions, the definition of lobbying activity is extended to cover efforts to induce rule making by executive branch agencies or other official actions of agencies, including the decision to enter into a contract or other arrangement.

The Company encourages its Personnel to take an active role in government processes. However, any participation in a political process is to be undertaken as an individual and not as a representative of the Company. Do not engage in lobbying activities on behalf of the Company without prior consultation with the Chief Executive Officer and Chairman.

Confidentiality

In the course of the Company's business, you will have access to business or personal information about the affairs of the Company, its clients, Personnel, suppliers and our business partners. It may include business strategies, competitive analysis, financial plans and forecasts, employee information, supplier information and pricing.

Each of the parties expects the confidential nature of the information they have given in good faith to be respected.

You must keep confidential information acquired while you are with the Company, or acting on behalf of the Company, confidential, even after you leave or cease your engagement with the Company. The Company encourages Personnel to store business records and confidential information securely. Anyone who uses the Company's systems or has access to the Company information (including access through personal devices such as laptops or mobile devices) shares responsibility for the security of those systems and information and must protect Company property – including data, information and systems – from theft, carelessness, misuse, unauthorised access and vulnerability to cyber attack.

You must not access or request or make improper use of or transfer or disclose confidential information to anyone else except as required by your position or as authorised or legally required. If it inadvertently comes into your possession it should be returned immediately. If you are required by an authority to provide confidential information which has not been otherwise authorised, you must notify the Company Secretary.

See the Information & Cyber Security (ICS) Policy for more information.

Privacy

You must respect and safeguard the privacy of personal information held by the Company regarding its clients, suppliers, Personnel and others. If you have access to this information, you must ensure that it is collected, kept, disclosed, handled and used in a manner that complies with the Privacy Act 1998 (Cth), Australian Privacy Principles any other privacy and data protection laws that may apply and the Company Privacy Policy available on the Company's website.

Social media use

1. Personal Social Media Use:
    a. Employees are free to engage in personal social media activities on their personal time and personal devices.
    b. While participating in personal social media activities, employees should ensure that their actions and statements do not violate any laws, compromise the organisation's confidential information, or harm its reputation.
2. Professional Social Media Use:
    a. Employees representing the organisation through official social media accounts or in any professional capacity should adhere to the organisation's social media guidelines and branding standards.
    b. Professional social media use should align with the organisation's values, objectives, and code of conduct.
    c. Employees should exercise professionalism, respect, and discretion when expressing opinions or sharing content related to the organisation or its stakeholders.

3. Protection of Confidential and Proprietary Information:

    a. Employees should not disclose or share confidential or proprietary information of the organisation, its clients, partners, or employees on social media platforms.
    b. Confidential or sensitive information about the organisation should only be shared through official channels and with appropriate authorisation.
4. Respectful and Responsible Behaviour:
    a. Employees should interact on social media platforms with respect for others' privacy, dignity, and diversity.
    b. Harassment, bullying, discrimination, or any form of offensive or inappropriate behaviour is strictly prohibited.
    c. Employees should refrain from engaging in activities that may harm the organisation's reputation, including making defamatory statements, spreading false information, or engaging in negative or harmful online discussions.
5. Separation of Personal and Professional Identities:
    a. Employees should make a clear distinction between personal and professional social media accounts and exercise caution in the information they share publicly.
    b. When expressing personal opinions online, employees should clearly state that their views do not represent the organisation's official position.

Discrimination, bullying, harassment and vilification

In Australia, it is unlawful to discriminate on the basis of a number of protected attributes including age, disability, race, sex, intersex status, gender identity and sexual orientation in certain areas of public life, including education and employment.

The Company is committed to taking all reasonable steps to prevent all forms of discrimination and harassment by ensuring that our Personnel understand the types of behaviours that are not acceptable in our interactions. Discrimination, bullying, harassment or vilification in the workplace will not be tolerated by the Company. Any such conduct will be dealt with in accordance with Company policy.

Sexual harassment

Specifically in relation to sexual harassment, the Company aims to:
1. Eradicate sexual harassment in all forms;
2. Create a positive and inclusive workplace;
3. Affirm the Company’ss commitment to promoting a safe working environment that is free from sexual harassment;
4. Support team members to report sexual harassment;
5. Ensure compliance with the Company’s legal obligations.

Legislation

Under State and Federal legislation, sexual harassment is unlawful and strictly prohibited. Relevant Federal legislation includes the following:
1. Fair Work Act 2009 (Cth) (FW Act) and the Fair Work Regulations 2009 (Cth);
2. Sex Discrimination Act 1984 (Cth); and
3. Sex Discrimination and Fair Work (Respect at Work) Amendment Act 2021 (Cth) (Respect at Work Amendment Act).

Definitions

"The Company's environment" means any physical or virtual place made available or authorised by the Company's directors for official use in connection with the Company's activities, including:

1. The Company's offices (and any offsite locations used in the Company's activities); and
2. Online environments (including the Company's website, email, LinkedIn profile etc.).

"Sexual harassment" means any unwelcome sexual advance, unwelcome request for sexual favours or other unwelcome conduct of a sexual nature which makes a person feel offended, humiliated or intimidated, and where that reaction is reasonable in the circumstances. Example of sexual harassment include, but are not limited to:

1. Inappropriate physical contact, such as unwelcome touching;
2. Staring or leering;
3. Unnecessary familiarity, such as deliberately brushing up against you or unwelcome touching;
4. Suggestive comments or jokes;
5. Insults or taunts of a sexual nature;
6. Intrusive questions or statements about your private life;
7. Displaying posters, magazines or screen savers of a sexual nature;
8. Sending sexually explicit emails or text messages;
9. Inappropriate advances on social networking sites;
10. Accessing sexually explicit internet sites;
11. Requests for sex or repeated unwanted requests to go out on dates; and
12. Behaviour that may also be considered to be an offence under criminal law, such as physical assault, indecent exposure, sexual assault, stalking or obscene communications.

Behaviour that is enthusiastically consensual and based on mutual attraction, friendship and respect is not sexual harassment.

NB: An individual that causes, instructs, induces, aids or permits sexual harassment to occur can also be found to have engaged in inappropriate behaviour and also be found liable.

NBB: The Respect at Work Amendment Act recently amended the FW Act to further support that sexual harassment can constitute serious misconduct and a valid reason for termination of employment without notice.

"Victimisation" means where someone subjects, or threatens to subject, another person to any form of detriment on the ground that the other person has:

1. Made a complaint of sexual harassment;
2. Provided information or documents regarding a complaint of sexual harassment;
3. Reasonably asserted their rights, or supported someone else's rights, under applicable anti-discrimination legislation; and / or
4. Made an allegation that a person has acted unlawfully under applicable anti-discrimination legislation.

Victimisation does not cover situations where it is proven that both the allegation was false and that the allegation was not made in good faith.

Protocols

If you feel that you have been subjected to any form of unlawful conduct contrary to laws, you are strongly encouraged to speak up. The Company has a comprehensive complaint procedure for dealing with these issues, which is articulated below. The complaint procedure has numerous options available to suit the particular circumstances of each individual situation.

The Company treats all complaints seriously and in accordance with this Policy. We also reiterate that if any team member is in immediate need of protection or emergency assistance, they should contact 000 as soon as possible.

1. Confront the issue
    a. Team members covered by this Policy who believe they are the subject of sexual harassment should take action at the earliest possible opportunity.
    b. Where appropriate, the person should make the perceived perpetrator(s) aware that they find their behaviour offensive, unwelcome, unacceptable and that it needs to stop immediately.
        i. This approach is more suited to less serious allegations.
2. Report the issue
    a. If the behaviour continues, or if the complainant feels unable to speak to the respondent(s) directly (or feels unsafe), they should speak to their immediate manager or the directors (if the conduct involves their manager).
    b. The directors and the immediate manager will provide support in accordance with this Policy. The complainant's wishes will be taken into account when deciding on a course of action but will not be the determinative factor.
3. Informal Intervention
    a. Under the informal complaint procedure, there are a broad range of options for addressing the complaint. The procedure used to address the issue will depend on the individual circumstances of the case. Possible options include:
        i. The relevant director or immediate manager discussing the issue with the person against whom the complaint is made; and/or
        ii. The relevant director or immediate manager facilitating a meeting between the parties in an attempt to resolve the issue and move forward.
            1. The informal complaint procedure is more suited to less serious allegations that do not warrant disciplinary action being taken.

4. Formal complaints procedure
    a. The formal complaint procedure will generally involve a formal investigation of the complaint. Formal investigations may be conducted internally (i.e. by the immediate manager or the director or a person external to the Company, where appropriate and as determined by the Company).
    b. An investigation involves collecting information about the complaint and then making a finding based on the available information as to whether or not the alleged behaviour occurred. Once a finding is made, the investigator will make recommendations about resolving the complaint.
    c. If The Company considers it appropriate for the safe and efficient conduct of an investigation, team members may be required not to carry out their duties or attend the Company activities during an investigation. The Company may also provide alternative duties or tasks during an investigation.
    d. The findings as to whether the allegations have occurred will be determined on the basis of the evidence, and on the balance of probabilities.
    e. On the basis of the findings, possible outcomes of the investigation may include, but will not be limited to, any combination of the following:
        i. Counselling;
        ii. Disciplinary action against the respondent (i.e. demotion, transfer, suspension, probation, termination or cessation of engagement);
        iii. Restriction from being associated with Company activities;
        iv. Official warnings that are noted in the respondent's The Company file;
        v. Formal apologies and undertaking that the behaviour will cease; and/or conciliation/mediation conducted by an impartial third party where the parties to the complaint agree to a mutually acceptable resolution.
    f. On completion of the investigation, parties will be informed about the investigation findings and the outcome of the investigation.

Supports

The Company strongly encourages any survivor or witness of sexual harassment to speak to their immediate manager or the directors, who can offer supports and assistance.
If you feel unsafe or need immediate help, we also confirm that you can:

1. Call 000;
2. Call Lifeline on 13 11 14;
3. Call 1800Respect (national sexual assault hotline) on 1800 737 732; and/or
4. Speak to your local GP.

Diversity

The Company recognises that workplace diversity, including gender, age, ethnicity, cultural background, qualifications and experiences is a key contributor to our business success, and is committed to an inclusive, diverse and non-discriminatory workplace and approach to our activities. Diversity not only supports a positive social framework, but also leads to superior organisational performance and culture. We also respect shareholder diversity and diversity reflected in the communities in which we operate.

The Company encourages greater gender diversity; it is important to effectively nurture and develop the pool of potential available talent. Early identification and development of female talent is clearly of significant importance in ensuring that there are appropriately qualified and experienced women for consideration when positions become available.

The Company seeks to create an inclusive workplace that embraces and promotes diversity as part of our corporate culture. This involves providing supportive and inclusive diversity-related workplace policies, programs and practices within our business.

The Company aims to improve the diversity of staff over time by the following initiatives:

1. Recruit Personnel on the basis of merit, skills and qualifications, while having regard for diversity;
2. Examining factors relating to gender diversity in the past and analysing ways to improve;
3. Ensuring this policy is communicated to staff in all levels of the Company;
4. Prevent and stop bullying, discrimination and harassment;
5. Induction, training and other programs promoting diversity; and
6. Making the recruitment process accessible to all candidates by advertising positions both broadly and in specific publications, using professional recruitment services where required and providing guidance on its recruitment processes.

Health and safety

The Company is committed to ensuring the health and safety of its Personnel and visitors to its sites and any other persons who the Company works with, as required by law. You must comply with the laws and regulations that apply to the Company and its operations.

Company officers have additional due diligence health and safety obligations which they must comply with.

The use of alcohol and drugs may impair performance at work, have an adverse impact on productivity, and can pose a risk to health and safety. To assist with ensuring the safety of our workplace, the consumption of alcohol, and the use of any prescription drugs which may impair a person’s ability to perform their work, or which pose a risk to their or others’ health and safety, must be strictly in accordance with Company policy.

You must not knowingly participate in any illegal or unethical activity. The Company will not tolerate the use of illegal drugs or improperly used prescription medicine, or alcohol (except for moderate consumption at social events) on Company premises or when performing work for the Company, travelling on behalf of the Company, attending work related functions or activities or conducting business on the Company’s behalf.

The possession, use, sale or offering or distribution of illegal drugs or other controlled substances on Company premises or while performing work for the Company, conducting Company business, travelling on behalf of the Company or at work related functions or activities is forbidden.

It is important that we work together to create a safe and healthy workplace. If you know of or suspect any unsafe situations or conditions, please alert the Company Secretary immediately.

Protection and use of the Company's assets and property

You must protect the Company's assets and property (including intellectual property) and ensure that the Company's assets and property are used only for the benefit of the Company's business. You must report any suspected or actual theft or fraud to the Company Secretary or any other contact nominated by the Company.

You must not use the Company's assets or property for personal purposes except in accordance with any Company policy or approved arrangement.

You must return Company assets and property immediately upon request by the Company.

All expenses must be documented and reported in a timely manner.

Responsibility to shareholders and the financial community

The Company is committed to providing value to its shareholders and recognising the legitimate interests of other stakeholders. The Company has policies regarding the timely provision of information to its shareholders and other stakeholders including posting information to its website. It has processes to ensure that the accounts and financial information it provides represent a true and fair view of the financial performance and position of the Company.

You must fully cooperate with, and not make any false or misleading statement to, or conceal any relevant information from, the Company's auditors.

Insider trading

Insider trading laws prohibit a person in possession of material non-public information relating to a company from dealing in that company's securities. Insider trading is a serious offence under the Corporations Act.

The Company's Trading Policy is available on the Company's website. It provides guidance so that you do not deliberately or inadvertently breach the insider trading laws or the Company's policy.

Environmental responsibility

The Company considers both the environmental impacts and benefits of its decisions and business activities. The Company is committed to doing business in an environmentally responsible manner and identifying environmental risks that may arise out of its operations. Employees must abide by all local laws and regulations, and are expected to respect and care for the environment in which the Company operates.

Any Personnel who are aware of, or suspect, an action that is not environmentally responsible or in breach of the applicable laws and regulations, must contact the Company Secretary.

Whistleblower protection

You are encouraged to report any actual or suspected unethical behaviour including breach of the Company's codes and policies to the Company Secretary or any other contact nominated by the Company. Matters raised will be investigated.

The Company is committed to ensuring that you can raise concerns in good faith without being disadvantaged in any way to the extent that the law permits.

Recruitment referral

Referral bonus

The reward for a successful referral attracts a $4,000.00 AUD bonus which is paid in the following instalments:

1. $2,000.00 AUD due upon the commencement of the candidate; and
2. An additional $2,000.00 AUD is payable after the referred individual passes their 6 month probation.

The reward for a successful specialist role referral attracts a $10,000.00 AUD bonus which is paid in the following instalments:

1. $5,000.00 AUD due upon the commencement of the candidate; and
2. An additional $5,000.00 AUD is payable after the referred individual passes their 6 month probation.

A specialist role refers to a position within the organisation that requires in-depth knowledge, skills, or expertise in a specific field, domain, or area of work. Unlike generalist roles that encompass a broad range of responsibilities, a specialist role focuses on a particular niche or specialised function.

The referral payment is gross and will be subject to applicable superannuation and taxation. It will be processed in the subsequent pay period. For referrals of fixed term contracts between 6 and 12 months in duration, the referral bonus will be pro-rated according to the contract length outlined in the offer of employment.

Eligibility

Referrals are paid to an employee of the Company for referring a candidate that then becomes directly employed by the Company in either a permanent full time, permanent part time, or fixed term contract position (minimum 6 months).

Referred candidates will be accepted under the following circumstances:

1. They are not already working for the Company, nor have they worked for the Company during the last 12 months;
2. They have not been submitted to Identitii by a recruitment agency within the last 12 months; and
3. They have not applied directly or been referred by another employee within the last 6 months.

To avoid any conflicts of interest, the direct manager for the position, although encouraged to refer candidates, is not eligible to receive a referral bonus.

Staff screening

Ensuring the recruitment and integration of suitable individuals is crucial for the Company's success as it establishes the foundation of its culture. Conducting staff screening is imperative to establish uniformity in our recruitment and hiring procedures, mitigating hiring risks, preventing legal issues, and minimising operational expenses.

The Company has established guidelines and obligations for conducting background checks on Staff in order to:

1. Detect any efforts to hide pertinent details or present false information
2. Identify potential instances of internal misconduct and deceit
3. Furnish pertinent information for regulatory verifications, if applicable
4. Adhere to both financial and non-financial regulatory obligations

Appendix A outlines guidance regarding the screening checks that may be applied. Some checks may be applied for all candidates, and others only where the level of responsibility and associated risk is significant.

Staff onboarding, offboarding, and role changes

1. Onboarding (Joiners):
    a. The organisation is committed to providing a comprehensive onboarding process for all new employees, ensuring they receive the necessary information, resources, and support to integrate smoothly into their roles.
    b. Onboarding programs will include orientation sessions, job-specific training, introductions to key team members, and access to relevant systems and tools.
2. Offboarding (Leavers):
    a. The organisation recognizes the importance of a well-managed offboarding process to conclude the employment relationship in a respectful and orderly manner.
    b. Offboarding procedures will include necessary exit interviews, revocation of system access, return of company property, and the completion of required paperwork or documentation.

3. Role Changes (Movers):
    a. The organisation acknowledges that role changes, including promotions, transfers, or reassignments, can be significant milestones in an employee's career progression.
    b. Role change processes will be structured to ensure transparency, fairness, and effective communication between employees, supervisors, and relevant stakeholders.
    c. Role changes processes shall take into account information security considerations in relation to access permissions and information asset handling.
4. Communication and Documentation:
    a. Clear and timely communication will be provided to employees regarding the onboarding, offboarding, or role change processes.
    b. All relevant documentation, such as employment contracts, confidentiality agreements, or performance evaluations, will be appropriately maintained and updated during these transitions.
5. Training and Support:
    a. Employees involved in the onboarding, offboarding, or role change processes will receive the necessary training, resources, and support to effectively carry out their responsibilities.
    b. Training may include guidelines on conducting exit interviews, onboarding new employees, or facilitating smooth role transitions.
6. Compliance and Confidentiality:
    a. Onboarding, offboarding, and role change procedures will adhere to applicable legal requirements, organisational policies, and confidentiality obligations.
    b. Employee privacy and the protection of sensitive information will be upheld throughout these processes.
7. Continuous Improvement:
    a. The organisation is committed to continuously evaluating and enhancing the onboarding, offboarding, and role change processes based on employee feedback, industry best practices, and evolving business needs.
    b. Feedback from employees and relevant stakeholders will be sought to identify areas for improvement and to ensure a positive experience during these transitions.

Worker rights and responsibilities

If you are a temporary working visa holder, a permanent resident, or an Australian citizen, you are covered by work health and safety laws. These laws apply to every workplace. For employees located in an overseas office the relevant equivalent standard in your location will apply.

Your basic rights include:

1. The right to be shown how to work safely.
2. The right to appropriate safety equipment.
3. The right to speak up about work conditions.
4. The right to say no to unsafe work.
5. The right to be consulted about safety in the workplace.
6. The right to workers compensation.
7. The right to a fair and just workplace.
8. The right to fair pay and conditions.

You also have specific health and safety obligations and responsibilities including:

1. Taking reasonable care of yourself.
2. Not doing anything that would affect the health and safety of others at work.
3. Following any reasonable health and safety instructions from your employer.

It is important that you:

1. Ask if you are not sure how to safely perform the work.
2. Follow instructions and work safely.
3. Report unsafe and unhealthy situations and injuries to your immediate supervisor.

Health and safety representatives or your supervisor can take your health and safety issues to your employer on your behalf. If you work through a group training organisation or labour hire agency, you can also report any work health and safety concerns to them.

For further guidance refer to the relevant employment relations body within your jurisdiction.

Health and wellbeing

1. Physical Wellbeing:
    a. Regular exercise can help to reduce anxiety and build up your tolerance for stress.
    b. We encourage staff to have walking or standing meetings where possible.
    c. Whilst some meetings, which require laptops or are with customers, are better suited for a formal setting, there are a number of meetings which could be taken outside or standing up.
2. Mental Wellbeing:
    a. All employees and their immediate family members have access to our Employee Assistance Program (EAP) service, which is a private and confidential one-on-one counselling service delivered by qualified psychologists.
    b. This service is available 24/7.
    c. The EAP can be used for assistance with any problems, work related or personal which may affect the work performance, safety or health of our staff.
    d. The Company EAP provider is Acacia. You can contact them directly on: 1300 364 273. Further information can be found through their website: www.acaciaconnection.com
3. Mental Health Days:
    a. All permanent employees receive 10 days personal/carers leave each year (pro-rated for part-time employees).
    b. To ensure you have an adequate balance staff are allowed to take up to 5 days of this leave as mental health leave, and the other 5 as personal or carer’s leave.
    c. If you require more than 5 days off per calendar year for your mental health, please speak to your Manager.

4. Social Wellbeing & Community:
    a. We celebrate employee achievements and success. This is an opportunity for peers to "shout out" a colleague for any special achievements or contributions made.
    b. The Company holds regular social events for all employees to attend and enjoy, including:
        i. Social employee drinks throughout the year
        ii. Team lunches throughout the year
        iii. Quarterly team building events
        iv. Christmas party event
        v. Other ad hoc offsite team building activities
5. Wellbeing Allowance:
    a. Upon commencement with the Company, all staff are eligible to claim a monthly wellbeing allowance of $100 AUD.
    b. Full-time and part-time staff are entitled to receive the same allowance, and it is not pro-rated based on hours of work.
    c. This allowance resets at the end of each calendar month and does not accumulate or roll over if unused. It can not be used in advance.
    d. To claim your wellbeing allowance, you must submit your receipts to Accounts before the end of the month for payment within the next pay cycle.
    e. All receipts must be submitted no longer than 1 month after the month it is incurred for payment to be made.
    f. Examples of items that can be claimed are:
        i. Spas, massages or facials
        ii. Acupuncture
        iii. Gym classes, apps and/or memberships
        iv. Yoga or meditation classes, courses or applications
        v. Workout or sporting equipment or wear
        vi. Chiropractor or physiotherapist
        vii. Psychologist or Psychiatrist
        viii. Nutritionist or naturopath
        ix. Health supplements
        x. Essential oils
        xi. Sporting activities including golf
        xii. Personal development books or other resources
        xiii. Any online application related to wellbeing – e.g. mindfulness, meditation, relaxation, breathing techniques
    g. Examples of items that cannot be claimed are:
        i. Alcohol
        ii. Food
        iii. Costs relating to a trip or holiday
        iv. Costs related to social activities
        v. Travel costs and expenses
        vi. Everyday clothing or makeup
        vii. Homewares
        viii. Private health insurance policies
        ix. Xbox, play station, or other gaming devices

Family and domestic violence leave

Definitions

"Family and domestic violence" means violent, threatening or other abusive behaviour by certain individuals known to an employee that both:

1. Seeks to coerce or control the employee.
2. Causes them harm or fear.

A "close relative" is:

1. An employee's:
   a. Spouse or former spouse
   b. De facto partner or former de facto partner
   c. Child
   d. Parent
   e. Grandparent
   f. Grandchild
   g. Sibling
2. An employee's current or former spouse or de facto partner's child, parent, grandparent, grandchild or sibling, or
3. A person related to the employee according to Aboriginal or Torres Strait Islander kinship rules.

Access

Employees must be experiencing family and domestic violence to be eligible to take paid family and domestic violence leave. To access paid family and domestic violence leave, the individual could be:

1. An employee's close relative
2. A member of an employee's household, or
3. A current or former intimate partner of an employee.

To access unpaid family and domestic violence leave, the individual needs to be a close relative.

All employees can access up to 10 days of paid family domestic violence leave leave each year. This includes full-time, part-time and casual employees. All employees are entitled to 5 days of unpaid family and domestic violence leave each year. This includes part-time and casual employees.

The entitlement to paid or unpaid family and domestic violence leave comes from the National Employment Standards (NES). It's a minimum leave entitlement, like annual leave or sick and carer's leave. Employees are entitled to the full 10 days upfront (i.e. on 1 February 2023 or for new starters, their first day), meaning you won't have to accumulate it over time. Family & domestic violence leave doesn't accumulate from year to year if it isn't used. Instead, the leave renews in full every year on each employee's work anniversary.

Disbursement

Family & domestic violence leave is paid:

1. Paid Family & Domestic Violence Leave for an employee other than a casual – at the employee's full rate of pay, worked out as if the employee had not taken the period of leave; or
2. For a casual employee – at the employee's full rate of pay, worked out as if the employee had worked the hours in the period for which the employee was rostered (NB: casuals can still take family & domestic violence leave for hours which they were not rostered to work, but they won't be paid in relation to such a period).

Protections

The Company will take all reasonable steps to ensure you are provided with a safe workplace and that any information provided to us is treated sensitively and confidentially. For example, if you were to disclose that you are affected by family or domestic violence,the director or manager will:

1. Make themselves available to talk with you as a matter of priority if you would like to;
2. Discuss your workplace entitlements and options available to you, such as taking family & domestic violence leave or accessing flexible work arrangements;
3. Discuss possible safety measures that could be implemented, such as screening the employee's incoming calls, blocking emails, changing a phone number, or changing working hours or location; and
4. Take steps to ensure all disclosures and activities are kept confidential.

The Company will also ensure that:

1. There is a zero tolerance to victimising any survivor for taking family & domestic violence leave (NB: if you have any concerns of victimisation please report this to a director or manager as soon as possible); and
2. In line with the NES, pay slips will not mention family & domestic violence leave, including any leave taken and leave balances.

Supports

The Company strongly encourages any survivor or witness of family & domestic violence to speak to their immediate manager or the directors, who can offer support and assistance. If you feel unsafe or need immediate help, we also confirm that you can:

1. Call 000;
2. Call 1800Respect (Australia's national sexual assault, domestic and family violence support service) on 1800 737 732;
3. Call safe steps Family Violence Response Centre (crisis response phone line) on 1800015 188;
4. Call Lifeline on 13 11 14;
5. And/or speak to your local GP.

Further information on various supports can also be found here.

Flexible and remote work

1. Remote Work:
    a. The organisation acknowledges the potential benefits of remote work arrangements and may consider granting employees the opportunity to work remotely, subject to the nature of their roles, performance, and business needs.
    b. Remote work arrangements should be based on mutual agreement between employees and their respective managers, ensuring that job responsibilities and performance standards can be effectively met.
    c. Employees working remotely are expected to adhere to the same policies, procedures, and standards as in-office employees, including maintaining confidentiality, data security, and professional conduct.
2. Flexible Work:
    a. The organisation recognises the value of flexibility in work schedules to accommodate personal needs and responsibilities while fulfilling work obligations.
    b. Flexible work arrangements, such as flexible start and end times or compressed workweeks, may be considered based on operational requirements and individual circumstances.
    c. Employees seeking flexible work arrangements should discuss their needs with their supervisors or HR representatives, ensuring that these arrangements align with team objectives and customer service requirements.
3. Working from Home:
    a. Working from home may be permitted in cases where employees require occasional flexibility or face temporary circumstances that prevent them from working at the office.
    b. Requests to work from home should be communicated to supervisors in advance, indicating the reasons, duration, and any necessary arrangements to ensure continuity of work and customer service.
    c. Employees working from home are responsible for maintaining a suitable workspace, adhering to health and safety guidelines, and ensuring productivity and accessibility during agreed-upon working hours.
4. Communication and Collaboration:
    a. Employees engaged in remote work, flexible work, or working from home should actively participate in communication and collaboration platforms provided by the organisation to ensure effective team coordination, information sharing, and project management.
    b. Regular communication with supervisors and team members is essential to maintain alignment, provide updates, and address any challenges or concerns promptly.
5. Evaluation and Adjustments:
    a. Remote work, flexible work arrangements, and working from home will be subject to periodic evaluation to ensure their effectiveness, impact on productivity, and alignment with organisational goals.
    b. The organisation reserves the right to adjust or revoke remote work or flexible work arrangements based on operational needs, performance considerations, or changes in circumstances.

All flexible work, remote work, and working from home arrangements are subject to the Remote and Flexible Work Standard.

Continuous competence development

1. Commitment to Continuous Competence Development:
    a. The organisation is committed to creating a culture that values continuous learning and professional development.
    b. Employees are encouraged to actively participate in competence development activities to enhance their skills, knowledge, and capabilities.
2. Training and Learning Opportunities:
    a. The organisation may provide a range of training programs, workshops, seminars, and online learning resources to support employees' professional development.
    b. Training opportunities will be aligned with job requirements, organisational needs, and individual development plans.
    c. Employees are encouraged to engage in self-directed learning, seeking relevant resources and external courses to complement the organisation's training offerings.
3. Career Advancement Programs:
    a. The organisation may establish career advancement programs designed to identify and nurture high-potential employees, providing them with opportunities for growth and advancement within the organisation.
    b. Career advancement programs may include mentorship initiatives, job rotation, leadership development programs, or succession planning processes.
4. Individual Development Plans:
    a. Employees will have the opportunity to collaborate with their supervisors or designated mentors to create individual development plans.
    b. Individual development plans should outline employees' career goals, areas for improvement, and steps to acquire the necessary skills and knowledge.
    c. Regular review and updates of individual development plans should occur to ensure alignment with changing job requirements and organisational priorities.
5. Support and Resources:
    a. The organisation will allocate appropriate resources, including time, budget, and technology, to support employees' competence development efforts.
    b. Employees may have access to learning platforms, online libraries, relevant industry publications, and other resources to facilitate their learning journey.
6. Recognition and Rewards:
    a. The organisation may recognise and reward employees who actively engage in competence development activities and demonstrate continuous improvement in their skills and capabilities.
    b. Recognition may include performance evaluations, career progression opportunities, monetary rewards, or other forms of acknowledgment.
7. Evaluation and Feedback:
8. The organisation will periodically assess the effectiveness of competence development initiatives and seek feedback from employees to ensure their relevance and impact.
9. Continuous improvement efforts will be made based on evaluation outcomes and feedback received.

Delegation of authority

The delegation of authority:

1. Defines Board of Directors delegated authority and provide guidelines on its application;
2. Facilitates compliance with relevant directions from the CEO and/or Board of Directors;
3. Establishes the levels of authority delegated to duly appointed Officers, contractors and staff of the Company;
4. Details authority to incur expenditure and administer funds;
5. Clarifies accountability and responsibility for the day-to-day operations of the Company for the Board of Directors.
6. Applies to all Board of Directors, employees and contractors of the Company.

No amendments shall be made to the specified delegations without the approval of the Board of Directors.

Principles of delegation

1. All financial delegations are subject to the approved annual budget allocation. Any items outside the approved budget must be referred to the CEO.
2. All dollar values are in AUD unless otherwise written.
3. Dual authorisation is required for approvals where there is more than one approver for threshold amounts.
4. All Delegations are subject to any overriding federal/state legislation.
5. Consideration must be given to risks and internal controls when exercising a delegation.
6. The delegation of authority is unique to a specified position (or to a person acting in that position) and not transferable.
7. Monetary amounts (excluding GST) as stated in this policy are the maximum delegated amounts per transaction.
8. All expenditure is to be approved considering availability of funding within budget and expense area.
9. Approval must not be made for any self-related matters - these include expenditure or reimbursement to self, certifying own invoices, higher duty allowance, and any type of leave or amendments to salary packaging.
10. All amendments, changes and deletions to the Delegations Policy must be considered by C-Level and endorsed by the Board of Directors.

Agreements or contracts

The authority to sign contracts within the delegated authority limits and parameters of the approved budget is outlined in Appendix C - Schedule of Delegations. Contracts over the delegated limit must be approved by the Board of Directors.
Agreements and contracts that may infer legal rights and liabilities may relate to:

1. Agreements for the provision of goods and services - operational leases, computer services, software agreements etc.
2. Agreements for the receipt of goods and services
3. Engagement of consultants or agreements relating to consultants
4. Approval of transfer of assets
5. Approval of leases
6. Licences to use Company assets (Copyright)
7. Memoranda of Understanding

Policy implementation

Responsible parties involved in implementation

Role	Responsibilities
The Board	• Review and approve measurable objectives for achieving diversity, including gender diversity. • Assess these objectives from time to time and the progress in achieving. • Review and monitor the effectiveness of this policy.
Nomination and Remuneration Committee	• The Board has delegated to the Nomination and Remuneration Committee the role of overseeing the implementation of certain parts of this policy. • The Nomination and Remuneration Committee will annually assess the Company's measurable objectives and its progress in achieving them.
Company Secretary	• The Company Secretary is designated as the responsible individual for overseeing the administration of the code of conduct. As of the adoption date of this code, the Company Secretary assumes this role. • It is the responsibility of the Company Secretary to provide guidance and support to individuals who require additional information, assistance, or have any uncertainties regarding the application of the code of conduct or related legal matters.

People Operations	• Develop, update, and communicate the policy to all employees. • Provide guidance and support to employees and managers regarding policy interpretation and implementation. • Monitor and assess policy compliance across the organisation. • Investigate policy violations, complaints, and concerns. • Administer disciplinary actions or corrective measures as required. • Collaborate with other departments to ensure consistent policy enforcement. • Act as a point of contact for employees and managers regarding policy-related queries and concerns. • Collaborate with line managers to ensure policy understanding and implementation within their teams. • Provide training and awareness sessions on policy requirements and expectations. • Support line managers in addressing policy-related issues or conflicts within their teams. • Assist in investigating and resolving policy violations or complaints.
Compliance	• Ensure that the People & Culture policy aligns with relevant laws, regulations, and industry standards. • Conduct regular audits or reviews to assess policy adherence and identify potential gaps or risks. • Develop and implement monitoring mechanisms to track policy compliance across the organisation. • Collaborate with People Operations and other stakeholders to address policy violations and implement corrective actions. • Stay updated on changes in laws or regulations that may impact policy requirements. • Provide guidance and expertise on compliance matters related to the policy.

Legal	• Review and ensure the People & Culture policy is legally compliant and aligns with applicable laws and regulations. • Provide advice and guidance on legal implications related to policy enforcement and disciplinary actions. • Collaborate with People Operations and Compliance departments to address policy violations and mitigate legal risks. • Stay informed about changes in employment laws or regulations that may impact the policy.

Communication and distribution

To ensure effective communication of the policy to relevant stakeholders, the following steps can be taken:

1. Distribution and Accessibility:
    a. The policy document should be made available to all relevant stakeholders in a centralised and easily accessible location. This could be achieved by publishing the policy on the organisation's intranet, document management system, or employee portal.
    b. Additionally, stakeholders should be notified about the availability of the policy and provided with instructions on how to access it.
2. Training and Awareness Programs:
    a. Conduct training sessions or workshops to educate stakeholders about the policy and its importance.
    b. These sessions can include presentations, interactive discussions, and practical examples to enhance understanding.
    c. Ensure that all employees, including executives, managers, and staff in different roles, attend the training sessions.
    d. It is also important to conduct periodic refresher training to reinforce key policy concepts.
3. Acknowledgement and Acceptance:
    a. Require stakeholders to acknowledge their understanding and acceptance of the policy. This can be done through the implementation of an electronic or physical acknowledgement process where stakeholders sign or electronically acknowledge that they have read and understood the policy. This ensures that stakeholders are aware of their responsibilities and are accountable for complying with the policy.
4. Communication Channels:
    a. Utilise various communication channels to reinforce the policy's message and updates.
    b. These channels can include internal newsletters, email communications, team meetings, and notice boards.
    c. Regularly communicate updates or changes to the policy, and emphasise the importance of adhering to the policy's guidelines.

5. Ongoing Support and Guidance:
    a. Establish a designated point of contact, such as a security officer or a dedicated security team, to address stakeholders' questions, provide guidance, and offer support related to the policy. This ensures that stakeholders have access to the necessary resources and assistance to comply with the policy.
6. Integration into Onboarding Process:
    a. Incorporate the policy into the onboarding process for new employees.
    b. During orientation, provide an overview of the policy, explain its relevance to their role, and highlight the expectations for compliance.
    c. Provide access to the policy document and ensure that new employees acknowledge their understanding and acceptance of the policy.
7. Periodic Policy Review:
    a. Regularly review the policy to ensure its effectiveness and relevance in addressing evolving threats and technologies.
    b. Engage stakeholders in the review process by soliciting feedback and incorporating their insights and experiences into policy updates.
    c. Communicate any changes or revisions to the policy to all stakeholders in a timely manner.

Policy change requests

The process for requesting a change to the policy may typically involve the following steps:

1. Identify the Need for Change
    a. Any stakeholder who identifies the need for a change to the policy should carefully evaluate the rationale behind it. This may include new security risks, regulatory changes, technological advancements, or feedback received from employees, auditors, or other relevant sources.
    b. It's important to clearly articulate the reasons for the proposed change.
2. Document the Proposed Change:
    a. The stakeholder requesting the change should document the proposed modifications to the policy. This includes detailing the specific sections or clauses that require revision, addition, or removal, along with a clear explanation of the desired changes and the expected outcomes.
3. Impact Assessment:
    a. The proposed change should undergo an impact assessment to evaluate its potential consequences. This assessment may involve considering the impact on existing processes, procedures, technical controls, resources, and compliance requirements.
    b. It's crucial to assess both the positive and negative implications of the change.
4. Consultation and Collaboration:
    a. The stakeholder should engage in consultation and collaboration with relevant parties to gather input and feedback. This may include discussions with members of the information security team, legal counsel, risk management personnel, and other subject matter experts. Their expertise and perspectives can help evaluate the viability and effectiveness of the proposed change.
5. Review and Approval Process:
    a. The proposed change should undergo a formal review process, which may involve a designated committee or a specific individual responsible for policy management.

    b. The review process evaluates the proposed change in light of the organisation's goals, compliance requirements, and overall risk posture.
    c. The approval authority, such as the CTO or the Head of Operations, assesses the proposed change and decides whether to approve, reject, or request further modifications.
6. Communication and Documentation:
    a. Once the change is approved, it should be communicated to all relevant stakeholders. This includes updating the policy document with the revised sections or incorporating an addendum to the existing policy.
    b. The updated policy should be made easily accessible to all stakeholders through the organisation's established communication channels.
7. Training and Awareness:
    a. Conduct training or awareness sessions to educate employees about the revised policy. This ensures that all individuals affected by the change are aware of their new obligations and understand the reasons behind the modification.
    b. Training sessions may include explanations of the change, examples of its practical application, and clarification of any questions or concerns raised by employees.
8. Implementation and Monitoring:
    a. The revised policy should be implemented and enforced across the organisation.
    b. Ongoing monitoring and compliance assessments should be conducted to ensure adherence to the updated policy
    c. Any deviations or non-compliance should be addressed through appropriate corrective actions.

Policy exception process

Implementing a policy exception requires a careful evaluation and approval process to ensure that exceptions are justified, properly managed, and do not compromise the organisation.

The process for implementing a policy exception typically involves the following steps:

1. Identify the Need for an Exception:
    a. A stakeholder or individual within the organisation identifies a situation or circumstance that warrants an exception to a specific policy.
    b. The need for the exception must be clearly defined and supported by valid reasons, such as business requirements, technical limitations, or legal or regulatory obligations.
2. Documentation of the Exception Request:
    a. The stakeholder requesting the exception should document the details of the exception request. This includes specifying the policy or control from which the exception is sought, describing the reason for the exception, and providing any supporting evidence or documentation.
3. Evaluation and Risk Assessment:
    a. The exception request undergoes an evaluation and risk assessment process. This involves assessing the potential impact of granting the exception on the organisation's security, compliance, and overall risk posture.
    b. The evaluation should consider the severity of the identified risk, available mitigating controls, and alternative solutions to address the situation.

4. Review and Approval Process:
    a. The exception request is reviewed by the appropriate authority or committee responsible for policy governance and compliance. This may involve the information security team, risk management personnel, legal counsel, or other relevant stakeholders.
    b. The review assesses the justification, feasibility, and acceptability of the requested exception.
    c. The approval authority makes a decision to approve, reject, or request further modifications to the exception request.
5. Documentation and Tracking:
    a. Once the exception is approved, it should be properly documented, including the justification for the exception, the approval details, and any conditions or limitations associated with the exception. This documentation helps ensure transparency, accountability, and auditability.
    b. The exception request and its approval status should be tracked in a centralised repository or system for future reference and reporting.
6. Communication and Awareness:
    a. The approved exception should be communicated to the relevant stakeholders who are affected by the exception. This includes notifying individuals responsible for implementing or enforcing the policy, as well as any other personnel who may be impacted by the exception.
    b. It's essential to ensure that all affected parties understand the scope, limitations, and duration of the exception.
7. Monitoring and Review:
    a. The exception should be periodically reviewed to assess its ongoing relevance and validity. This includes monitoring the associated risks, evaluating any changes in the organisation's environment, and reassessing the need for the exception.
    b. If circumstances change, the exception may be modified, extended, or revoked based on the reassessment results.
8. Reporting and Accountability:
    a. The exception process should include reporting mechanisms to ensure proper oversight and accountability. This may involve regular reporting to senior management, the board of directors, or other governing bodies to provide visibility into the exceptions granted and their associated risks.

Policy compliance and enforcement

Examples of non-compliance

Misconduct

Misconduct refers to actions or behaviour by an employee that deviates from the expected standards of conduct outlined in corporate policies or codes of conduct. It typically involves violations of company policies, rules, or guidelines, which may result in minor breaches or disruptions in the workplace.

Examples of misconduct include:

1. Minor policy violations:
    a. These can include tardiness, unauthorised personal use of company resources, or failure to adhere to dress code policies.
2. Insubordination:
    a. Disrespectful behaviour towards superiors or refusal to follow reasonable instructions falls under misconduct.
3. Non-compliance:
    a. Failure to adhere to specific procedures or protocols outlined by the organisation, such as timekeeping or reporting requirements.
4. Minor conflicts of interest:
    a. Engaging in activities that may compromise the employee's objectivity or create a conflict between personal and professional interests.

Serious misconduct

Serious misconduct refers to actions or behaviour that significantly and detrimentally impact the organisation, its employees, clients, or stakeholders. It involves more severe violations that breach ethical standards, cause harm, or disrupt the workplace environment. Serious misconduct may have legal implications and can result in immediate termination of employment. Examples of serious misconduct include:

1. Theft or fraud:
    a. Engaging in fraudulent activities, embezzlement, misappropriation of company funds, or stealing company property.
2. Workplace violence or harassment:
    a. Physical assault, threats, intimidation, or any form of harassment that creates a hostile or unsafe work environment.
3. Gross negligence or recklessness:
    a. Engaging in actions that pose a significant risk to the safety of others or the company's operations, such as deliberate sabotage or deliberate violations of safety protocols.
4. Discrimination:
    a. Treating others unfairly based on protected characteristics, such as race, gender, religion, or disability.
5. Breach of confidentiality:
    a. Unauthorised disclosure of confidential or sensitive information, including client data or trade secrets.

Consequences for non-compliance

While misconduct is considered a breach of company policies, it is typically addressed through disciplinary measures or corrective actions, such as verbal warnings, written warnings, counselling, or performance improvement plans.

Due to the severe nature of serious misconduct, immediate and decisive action is often taken, including disciplinary proceedings, investigations, termination, and potential legal consequences.

Policy monitoring and evaluation

Monitoring and evaluation

Monitoring and evaluating the progress and effectiveness of the policy is crucial to ensure its continuous improvement and alignment with organisational goals. Monitoring and evaluation may be conducted through internal audit, external audit, and manual audits of controls:

1. Internal Audit:
    a. Internal audit teams or personnel, independent from the areas being audited, can assess the implementation and compliance of the policy.
    b. Internal audits can include a review of security controls, processes, and procedures to determine their effectiveness and identify any gaps or weaknesses.
    c. Internal auditors can conduct regular audits based on an audit plan, which outlines the areas to be audited and the frequency of audits.
    d. The internal audit function can evaluate the organisation's adherence to the policy's requirements, identify areas of non-compliance, and provide recommendations for improvement.
    e. The internal audit team may also assess the effectiveness of incident response processes, risk management practices, and security awareness and training programs.
2. External Audit:
    a. External audit firms or independent assessors can be engaged to evaluate the organisation's compliance with relevant standards, regulations, or industry best practices.
    b. External audits provide an objective assessment of the organisation's security controls and compliance with external requirements.
    c. External auditors may review the organisation's policies, procedures, and controls, and assess their effectiveness in achieving the desired security objectives.
    d. External audits can also provide an independent assessment of the organisation's data privacy and protection practices, including compliance with applicable privacy laws and regulations.
3. Manual Audits of Controls:
    a. Manual audits of controls involve conducting specific assessments of individual security controls and processes.
    b. These audits can be performed by designated individuals or teams responsible for managing specific controls, such as access control, network security, or data classification.
    c. Manual audits assess the adequacy and effectiveness of controls, identify any deviations or non-compliance, and recommend corrective actions.
    d. The audits can be conducted through interviews, documentation review, observations, and testing of control effectiveness.
    e. Manual audits help ensure that controls are properly implemented, monitored, and aligned with the policy's requirements.

4. Key Considerations:
    a. Monitoring and evaluation efforts should be based on a well-defined audit plan or schedule to ensure regular assessments of different aspects of the policy.
    b. The results of audits, both internal and external, should be documented and shared with relevant stakeholders, such as senior management.
    c. Identified gaps or non-compliance should be addressed through corrective actions and follow-up audits to verify the effectiveness of remedial measures.
    d. Monitoring and evaluation processes should be adaptable to changes in the organisation's environment, emerging threats, and evolving security requirements.
    e. It is important to ensure that auditors and assessors possess the necessary expertise and knowledge to effectively evaluate the policy and associated controls.

Review

To ensure the policy remains up-to-date, effective, and aligned with organisational goals, feedback, review, and periodic revisions should be incorporated into the policy management process. Here are mechanisms that can be implemented for these purposes:

1. Feedback Mechanisms:
    a. Establish a designated point of contact, such as a security officer or a dedicated security team, to receive feedback and suggestions regarding the policy.
    b. Encourage stakeholders to provide feedback through various channels, such as a designated email address, feedback forms, or an anonymous reporting system.
    c. Conduct surveys or focus group discussions to gather insights and perspectives from employees, management, and other stakeholders.
    d. Establish a culture of open communication and encourage stakeholders to proactively raise concerns or provide suggestions related to the policy.
2. Periodic Review:
    a. Define a timeline or schedule for conducting periodic reviews of the policy. The frequency may vary depending on the organisation's needs, but typically ranges from annually to biennially.
    b. Form a review committee consisting of representatives from relevant departments, such as information security, legal, compliance, and risk management, to conduct the policy review.
    c. During the review, assess the policy's alignment with emerging threats, changes in regulatory requirements, technological advancements, and lessons learned from incidents or audits.
    d. Solicit feedback from stakeholders during the review process to gather insights on the policy's strengths, weaknesses, and areas for improvement.
    e. Evaluate the policy against industry best practices, standards, and guidelines to ensure its relevance and effectiveness.

3. Revisions and Updates:
    a. Based on the feedback and findings from the review process, initiate the necessary revisions and updates to the policy.
    b. Clearly document all changes made to the policy, including the rationale and considerations behind each revision.
    c. Ensure that the revised policy reflects the latest security practices, addresses identified gaps or weaknesses, and incorporates new legal or regulatory requirements.
    d. Communicate the revisions to all stakeholders through appropriate channels, such as internal newsletters, email communications, or training sessions.
    e. Ensure that stakeholders have access to the updated policy document and are aware of the changes made.
4. Training and Awareness:
    a. Conduct training sessions or awareness programs to educate employees and stakeholders about the revised policy and its implications.
    b. Highlight the changes made, the reasons behind the revisions, and any new responsibilities or requirements resulting from the updated policy.
    c. Reinforce the importance of adhering to the policy and provide guidance on how to comply with the revised guidelines.
    d. Offer refresher training periodically to reinforce key policy concepts and maintain awareness among stakeholders.

Conclusion

The People & Culture Policy serves as a comprehensive guide to managing one of our organisation's most valuable assets—its people. Throughout this policy, we have outlined the key areas that impact our employees' experiences, from recruitment to offboarding and everything in between. By summarising the main points of this policy outline, we have established a framework that promotes fairness, inclusion, professional development, and well-being for all our staff members.

It is crucial to recognize the importance of this policy and the potential impact it can have on our organisation. By adhering to the principles and requirements outlined within this policy, we create a work environment that fosters respect, diversity, and collaboration. It sets clear expectations for behaviour, ethics, and professionalism, ensuring that all employees understand their rights and responsibilities. Furthermore, this policy empowers our line managers to lead and support their teams effectively, promoting employee engagement and development.

The implementation of this policy reinforces our commitment to creating a positive work culture that attracts and retains top talent. By valuing diversity, providing growth opportunities, and promoting work-life balance, we strive to enhance employee satisfaction, productivity, and loyalty. Our People & Culture Policy reflects our dedication to maintaining legal compliance, ethical conduct, and a supportive work environment where everyone can thrive.

As we move forward, it is imperative that all staff members familiarise themselves with the policy, embrace its principles, and actively contribute to its success. We encourage open communication, reporting any concerns, and engaging in continuous learning and development. By working together to uphold this policy, we can create an environment that fosters individual and organisational success.

In conclusion, the People & Culture Policy establishes a foundation for our organisation's approach to people management. It encompasses key areas such as recruitment, onboarding, diversity, performance, well-being, and more. By valuing and investing in our employees, we pave the way for a thriving and inclusive workplace that propels our organisation towards excellence.

Appendix A - Staff screening matrix

Role	Screening	Description
Board Members and Non-executive Directors	Bankruptcy	Information is obtained from the Australian Financial Security Authority (AFSA) and will include the following details: ● Type of administration or proceeding ● Date of administration or proceeding ● ID number ● Full name and alias of debtor ● Address of debtor ● Date of birth of debtor ● Occupation and business name of debtor ● Particulars of any prior or subsequent listing ● End date of the administration
	Business Interests	Information is obtained from the Australian Securities & Investments Commission (ASIC) and will include the following details: ● Name of any company they have been involved in ● Positions held ● Dates of appointment ● This check may also include Registration & Licensee information.
	Financial Regulatory	A Financial Regulatory Check will include a search from the following registers: ● ASIC's Banned and Disqualified Registers ● ASIC's Enforceable Undertakings Register ● APRA's Disqualification Register
	Anti Money Laundering	Anti Money Laundering (AML) check will conduct an online search of the following lists: ● Sanctions ● Law Enforcement ● Regulatory Enforcement ● High Profile Persons ● Politically Exposed Persons (PEP) ● Others e.g. Companies House, Financial Action Task Force
	National Police Check	All Australian National Police Checks are: ● Recorded in compliance with spent conviction legislation (click here to find out more) ● Include any current pending charges that have been initiated by the police ● May include traffic convictions.

Financial managers / Finance professionals e.g. Chief Financial Officer (CFO), Finance Manager etc.	Bankruptcy	Information is obtained from the Australian Financial Security Authority (AFSA) and will include the following details: • Type of administration or proceeding • Date of administration or proceeding • ID number • Full name and alias of debtor • Address of debtor • Date of birth of debtor • Occupation and business name of debtor • Particulars of any prior or subsequent listing • End date of the administration
	Anti Money Laundering	Anti Money Laundering (AML) check will conduct an online search of the following lists: • Sanctions • Law Enforcement • Regulatory Enforcement • High Profile Persons • Politically Exposed Persons (PEP) • Others e.g. Companies House, Financial Action Task Force
	National Police Check	All Australian National Police Checks are: • Recorded in compliance with spent conviction legislation (click here to find out more) • Include any current pending charges that have been initiated by the police • May include traffic convictions.
	Professional Membership Check	Professional Membership Check will verify an individual's Australian membership directly with the professional organisation and will obtain the following details: • Type of membership held • Date joined • Current membership status.
	Business Interests	Information is obtained from the Australian Securities & Investments Commission (ASIC) and will include the following details: • Name of any company they have been involved in • Positions held • Dates of appointment • This check may also include Registration & Licensee information.

<table>
<tr><td rowspan="2"></td><td>Employment Verification</td><td>This employment history check will verify the following details:
Name of organisation the individual was employed by
Dates employed
Nature of employment (full time, part time, casual, contract etc)
Last position held
Reason for leaving</td></tr>
<tr><td>Employment Reference</td><td>15 performance/behavioural based questions that are designed to give essential information to assess a candidate's past job performance and capabilities.

The questionnaire covers the following 4 categories:
Candidate information
Technical skills
Interpersonal and communication skills
Personal attributes</td></tr>
<tr><td rowspan="3">All other staff</td><td>Employment Verification</td><td>This employment history check will verify the following details:
Name of organisation the individual was employed by
Dates employed
Nature of employment (full time, part time, casual, contract etc)
Last position held
Reason for leaving</td></tr>
<tr><td>Employment Reference</td><td>15 performance/behavioural based questions that are designed to give essential information to assess a candidate's past job performance and capabilities.

The questionnaire covers the following 4 categories:
Candidate information
Technical skills
Interpersonal and communication skills
Personal attributes</td></tr>
<tr><td>National Police Check</td><td>All Australian National Police Checks are:
Recorded in compliance with spent conviction legislation (click here to find out more)
Include any current pending charges that have been initiated by the police
May include traffic convictions.</td></tr>
</table>

Appendix B - Approval matrix for screening discrepancies

Check	Description	Severity	Action required	Approval
Bankruptcy	Positive match on bankruptcy, declared or undeclared, discharged or pending.	Major	Assess materiality.	CEO
Business Interests	Business interests in a director competitor or industry adjacent company	Major	Assess materiality.	CEO
Financial Regulatory	Any adverse records or irregular findings or pending investigations.	Major	Assess materiality.	CEO
Anti Money Laundering	Possible/Positive match found for Politically Exposed Person.	Major	Recommend rejection.	CEO
	Possible/Positive sanctions match	Extreme	Reject candidate.	N/A
National Police Check	Criminal conviction found, possible criminal, appeal pending.	Major	Assess materiality.	CEO
Professional Membership Check	Discrepancy in dates of attendance, grades, degree, course description etc.	Minor	Assess whether this is a case of dishonesty.	Hiring manager
	Cannot locate or no response from institution /professional body.	Minor	Discuss with the hiring manager.	Hiring manager
	No record of candidate, or membership not attained.	Major	Assess materiality.	CEO

Employment Reference	Cannot locate or no response from reference.	Minor	Discuss with the hiring manager.	Hiring manager
	Forged/fraudulent reference	Major	Assess materiality.	CEO
Employment Verification	Discrepancy in dates of employment, salary, title and reason for leaving.	Minor	Assess whether this is a case of dishonesty.	Hiring manager
	Cannot locate or no response from previous employer.	Minor	Discuss with the hiring manager.	Hiring manager
	Forged documents, contractual violations, termination for cause, no records etc.	Major	Assess materiality.	CEO

Appendix C - Delegation of authority

Authority to approve expenditure

Description	Expenditure/activity (excl. GST)	Authorisation required	Narrative/document required	Control
Operating Expenditure	Greater than $100,000	Board of Directors	To be recommended by C-Level. Approval by the Board, to be noted in the Board Meeting minutes	Briefing paper to Board of Directors
	Less than or equal to $100,000	CEO	To be recommended by the Senior Leadership Team	
	Less than or equal to $500	Head of Operations	To be recommended by the Senior Leadership Team and endorsed by the CEO	

Capital Expenditure >$40,000	Greater than $40,000 over budget	Board of Directors	A suitable business case to be recommended by Senior Leadership Team and endorsed by Board of Directors	
Capital Expenditure <$40,000	Less than or equal to $40,000 within budget	CEO	A suitable business case	
Rent/rates and outgoings	All costs	CEO/ CFO or Head of Operations	All invoices checked with leases	
Expense Reimbursement	Less than or equal to $500	Head of Operations	To be recommended by the Senior Leadership Team and endorsed by the CEO	
	Less than or equal to $1000	Finance	Request for: • Spending Form • Travel Expense • Claim Form	Per Diem expenses Sundry reimbursements

	Greater than $1000	CEO	Written approval from CEO and request for: • Spending Form • Travel Expense • Claim Form	

Banking and finance

Description	Expenditure/activity (excl. GST)	Authorisation required	Narrative/document required	Control
Allocation of funds to term deposits	All	Chairman of the Board Board of Directors CEO	Formal approval from Chair and Board of Directors, CEO to move funds.	Update Investment Register
Open bank accounts	All	CEO	Appropriate forms from bank	Update accounts system
Credit cards	All	CEO	Appropriate forms from financial institutions. Approval from Board of Directors	All Credit Card invoices matched to statement and authorised by delegated personnel
EFT payment file upload/direct credit upload	All	CEO Finance	As per policy	After all operational controls and authorisations completed
Refunds	All	CEO	Formal request for refund	Supporting documentation regarding refund

Annual Operating Budget	All	Board Authorisation	Approved budget template	All expenditure outside budget allocation must be recommended by the Senior Leadership Team and endorsed by Board of Directors
Loan/Financing Activities	All	Board Authorisation	Approval from Board of Directors	Signed Loan/Financing Document

Invoicing and debtors

Description	Expenditure/activity (excl. GST)	Authorisation required	Narrative/document required	Control
Issue invoices	All	Finance	Formal invoice	
Write off bad debts	All	Board of Directors	Briefing paper	Recommendation by CEO and endorsed by Board of Directors

Human resources and payroll

Description	Expenditure/activity (excl. GST)	Authorisation required	Narrative/document required	Control
Approve formal engagement offers, determine fee and sign contracts	All	C-Level Hire: Board Approval Below C-Level Hire: CEO	Contract Referee check	
Approve final warnings and cessation of contracts	N/A	CEO	Formal performance improvement plan	
Approve professional development expenses, including training and conference attendance	Within approved budget	CEO	Policy for professional development	As per approved budget
Approve of leave without pay or special paid leave	N/A	Senior Leadership Team	Formal written request	
Approve invoices for contractors	Within approved budget	CEO	Formal Contractor agreement	

Travel

Description	Expenditure/activity (excl. GST)	Authorisation required	Narrative/document required	Control
All domestic travel expenses	> $250	Senior Leadership Team CEO	Request in writing	
	< $250	N/A	Expense Claim	
All international travel expenses	> $500	CEO	Request in writing	
All international travel expenses	< $500	N/A	Request in writing	
Domestic travel	As per budget	Senior Leadership Team CEO	Request for: • Spending Form • Travel Expense • Claim Form	Economy class for all domestic travel
International travel	As per budget	Senior Leadership Team CEO	Request for: • Spending Form • Travel Expense • Claim Form	Economy class for all international travel

Authority to enter contracts

Description	Expenditure/activity (excl. GST)	Authorisation required	Narrative/document required	Control
Enter into a Non-Disclosure Agreement	N/A	Senior Leadership Team	Countersigned NDA Legal Approval	Legal Request Service Request
Enter into a service agreement	Greater than $100,000	Board of Directors	Briefing paper Formal contract	New Vendor Service Request
Enter into a service agreement	Less than or equal to $100,000	CEO	Formal contract	New Vendor Service Request
Enter into a service agreement	Less than or equal to $10,000	Senior Leadership Team	Formal contract	New Vendor Service Request

Other specific authorities

Description	Expenditure/activity (excl. GST)	Authorisation required	Narrative/document required	Control
Amend or vary any insurance cover	N/A	CEO	Briefing paper	Meet with insurance company or broker
Approve all insurance and telecommunication expenses	N/A	CEO	Internal report	
Approve sale, disposal, destruction or trade-in of hardware assets	Less than or equal to $25,000	Head of Operations CEO	Internal report	
Amend Delegations Policy	N/A	Board of Directors	Briefing paper	
Approve decision to tender for a major business opportunity	N/A	CEO	Briefing paper Business case	

Identitii Limited
ACN 603 107 044

Registered Office
The Commons
Mezzanine, 388 George Street
Sydney, NSW
Australia 2000

www.identitii.com