



Union Council Meeting

14 July 2019 -4pm
Hyatt Regency
161 Sussex Street, Sydney

MINUTES

The meeting was declared open at 4.10pm by Mark Sterrey in the chair.

Attendees

Gerard Hayes
Mark Sterrey
Lynne Russell
Bruce Rowling
William Oddie
Steven Fraser
Joan Catlin
Sharon Carney
Jeffrey Knee
Gillian Reilly
Bryan Billington
Laycombe Reilly

Alan Wilcock
Robert Aney
Toni Winters
Donna Riley
John Lawrence
Edalina Hondros
Sue McGuire
Darriea Turley
Mick Callinan

1. Observers/Proxies/Apologies:

Apologies: Mark Jay, Leigh Bush, John Jetty Dore, Andrew Teece, Leesa Franks, Josephine Peacock. **Observers:** Angela Nigro, Angela Brown

Resolution:	UC 08/2019
Moved:	M Callinan
Seconded:	E. Hondros

"That the observers/proxies/apologies be accepted and admitted to the meeting."

PUT AND CARRIED

2. Conflict of Interest, Related Party Transaction Disclosers and other Disclosures

NIL

3. Minutes of Previous Meeting/s (Attached)

3.1 Union Council Meeting Minutes held 27 March 2019

Resolution: UC09/2019
Moved: S Fraser
Seconded: P Reid

“That the minutes of the Union Council meeting 27 March 2019 be accepted.”

PUT AND CARRIED

4. Matters arising from the Minutes:
NIL

5. SECRETARIES REPORTS:

Verbal report to be presented, Gerard Hayes, Secretary:

Gerard Hayes addressed the Union Council and gave the following report. He has reported that we are nearing 40,000 members and have grown by 10% from last year. We are the only union that is growing at that rate and are predicting that we will have grown by 15% in the next year.

We now have a staff of 115 going from 49 staff in a six-year period, with that growth, last year we have identified the need for a HR Department which has proved to be very beneficial creating policies and procedures, putting systems into place with a lot more work still to be done.

We have also identified the need to develop our CRM, to enhance the marketing, communication and engagement with our members, to enhance public opinion, integrating into social media platforms, to be proactive with the membership identifying activity or lack thereof. The current system Memforce is based on the Salesforce Platform which is noted as being one of the best platforms in the world. It has many capabilities which the staff do not utilise to the full capacity. We have identified the need of employing a Business Analyst to help develop the CRM, train staff and any other avenues the union may need to undertake to reach its full potential and growth.

Gerard also reported that the Jackson trial commenced two weeks ago. Gerard was called as a first witness. It will now reconvene in October 2019.

Resolution: UC10/2019
Moved: L Twyford
Seconded: W Oddie

“That the Union Council accepts the Secretaries report.”

PUT AND CARRIED

6. CHIEF FINANCE OFFICER – FINANCE REPORTS

6.1 FY20 Budget and cashflow projections (business paper and attachment)

6.1 Resolution: That the HSU NSW/ACT/QLD Union Council discuss, review and adopt the budget cashflow projections for the 2020 financial year.

Resolution: UC11/2019
Moved: A Wilcock
Seconded: D Turley

6.2 Insurance Brokerage Tender (Business paper attached)

An Expression of Interest for Insurance Brokerage Services was recently conducted. This was to meet the requirement to market test contracts with external providers every three years. The attached paper outlines an overview of the tenders that presented to the Tender Committee.

PUT AND CARRIED

6.2 Resolution:

That the HSU NSW/ACT/QLD Union Council approves the engagement of Marsh as the insurance broker of the HSU insurance program to 2022. Further, that the Assistant Secretary/Treasurer is authorised to renew the insurance policies on expiry over the next three years based on advice from Marsh insurance brokers.

Resolution: UC12/2019
Moved: J Catlin
Seconded: B Billington

PUT AND CARRIED

7. AGENDA ITEMS

7.1 Health Services Union Staff Enterprise Agreement (Attached)

Staff were informed via email and meeting of proposed changes to HSU NSW Employee Agreement as listed below. An online vote sent to staff covered by the agreement confirmed 90% staff Yes vote on 28 June

Proposed offer is as follows:

1. 2.5% wage increases from July 1 every year for the next 3 years.
2. A .5% increase in super on existing levels from July 1 2019
3. A mental health plan gap payment for anyone needing to access counselling services under Medicare.
4. An increase from 2 to 4 weeks leave for the non-primary caregiver of a child in the first 12 months after birth and an additional 10 weeks on top of this if that same parent becomes the primary caregiver within the first 12 months.

5. Health and Wellbeing program will be expanded to include Quit smoking aids and programs such as sprays, chewing gum, patches and any other service aimed at assisting you to quit

7.1 Resolution: That HSU NSW/ACT/QLD Union Council consider the proposed HSU NSW employee agreement to operate from the first full pay period on or after 1 July 2019 and to remain in force for a period of three years expiring on the 30 June 2022.

Resolution: U13/2019
Moved: S Carney
Seconded: B Rowlings

PUT AND CARRIED

7.2 IT Security Policy (Attached)

As tabled at the March 27, 2019 Union Council Meeting Draft Policies and Procedures additionally the following Policy is now tabled for Council consideration:

- IT Security Policy

7.2 Resolution: That the HSU NSW/ACT/QLD Union Council adopts the IT Security Policy under Rule 40 Union Policies and Procedures and once adopted applies to all officers, employees and members of the HSU NSW/ACT/QLD.

Resolution: UC14/2019
Moved: G Reilly
Seconded: J Lawrence

PUT AND CARRIED

7.3 Office Fit out/Renovation

A recent audit by Axiom Group of the floor space of HSU offices on Level 2 showed that the floor space of 800 sq. metres is currently utilized by the current 51 staff. Standards of the floor space should house approximately 80 staff. A redesign of the space will not only enable for future growth but also enable open space and utilise light.

Resolution: That the Union Council consider and approve the Secretary to be able to spend up to \$500,000 on a refurbishment of Level 2 of 109 Pitt Street, after three quotes are obtained as per the Procurement Policy and Procedure

Resolution: UC15/2019
Moved: L Reilly
Seconded: R Aney

PUT AND CARRIED

7.4 CRM Proposal:

In line with HSU Policy on tendering and procurement, the Customer Relationship Management (CRM) software database was put out to the market via the SMH and Tenderlink. The current contract with Cotswold Concepts (Memforce) expires in October 2019. In order to give sufficient time to transition if that was the decision of the HSU, the tender process commenced in August 2018.

7.4 Resolution: That the Union Council endorses the recommendation of the Audit & Finance Committee to re-engage Cotswold Concepts. That the Assistant Secretary/Treasurer is approved to sign the contract for the Memforce system for a further three years to 2022. Further that an internal FTE position of Business Analyst be adopted into the HSU staffing structure and recruited for immediately.

Resolution: UC16/2019
Moved: T Winters
Seconded: D Riley

7.5 Appointment of Ombudsman

Resolution: That the HSU NSW/ACT/QLD Union Council endorse the appointment of Mr Chris Brown as the Ombudsman

Resolution: UC17/2019
Moved: L Reilly
Seconded: L Russell

PUT AND CARRIED

8. GENERAL BUSINESS:

8.1 A motion of support that the Council has overwhelming confidence in Gerard Hayes in his successful running of the Branch as his position as the Secretary of the HSU NSW/ACT/QLD Branch.

Resolution: UC18/2019
Moved: E Hondros
Seconded: D Turley

8.2 Steve Fraser raised that the Council investigate the possibility of a "Emergency Welfare Fund" for members in the case of emergency support for members and their families. He gave an example of the Police force which apparently paid for flights, accommodation etc. for their family when their grandson needed emergency hospitalisation. Council endorsed the investigation of something similar. Steve Fraser to come back with details to the Branch Committee of Management.

UC19/2019

Moved: R Aney

Seconded: B Rowling

PUT AND CARRIED

The meeting was declared closed by Mark Sterrey (President) at 17.45pm

Signed:  M Sterrey (President)
Date: 28.8.19

**Health Services Union NSW/ACT/QLD
Union Council Meeting
Business Paper**



**BUDGET & CASHFLOW PROJECTIONS
July 2019 to June 2020**

Detail

A new operating profit and cashflow forecast has been completed for HSU NSW for the 2020 financial year (01 July 2019 to 30 June 2020).

In summary:

- Over the 12-month period operating profit is forecasted at \$215,117. Total net cash outflows are estimated at \$833,107, with the closing cash balance 30 June 2020 projected to be \$7,533,107 (the opening cash at bank will be approximately \$6,700,000).
- Total revenue for the year is estimated at \$20,987,377 and total expenditure is estimated at \$20,772,260 (therefore net profit forecast of \$215,117).
- Capital expenditure for the financial year is estimated to be \$1,394,000 made up of:
 - Motor vehicle replacements & fleet increase (\$544k);
 - IT upgrades & replacements (\$100k);
 - HSU head office fitout changes (\$500k); and
 - Potential CRM implementation (\$250k).

Main factors to note in the budget are listed below:

- Membership contributions (\$19.06m) were estimated based on an average yearly level of 37,305 financial members (930 of which will go to the Branch but credited back as a service fee). While the actual level tends to be higher than this assumption, the income received fluctuates according to un-financial members, direct debit & credit card rejections, waivers and refunds. Net growth of 1,600 members has been phased in over the year. Previously growth has not been phased throughout the budget but this will demonstrate a more realistic approach to the contributions budget.
- Rental income for the properties (\$1.34m) is based on the current tenancy schedule over the period with contracted increases.
- Advertising revenue from the magazine estimated at (\$12k).

- Interest income is based on cash at bank over the period (including term deposits) of \$95k.
- Service fees from the Branch (\$380k) include income from ACT and QLD members less expenses for affiliations, capitation and the ACT office costs.
- Sponsorship income (of \$32k) is to be received for the annual delegates conference.
- Affiliation expenses (\$1.38m) include general subscriptions (\$55k) plus ACTU (\$238k), ALP (\$187k) and Unions NSW (\$135k) affiliation costs and the HSU National capitation fees (\$766k).
- The Annual Delegates Conference has been set at the Union Council approved budget of \$650k.
- Building costs (\$782k) are all associated payments with the rental portfolio, including property management fees and expenses associated with the Sydney Head office building.
- Campaign expenses have been budgeted at \$150k for the financial year.
- IT expenses (\$384k) include costs associated with the MemForce database, MCR IT managed services, Exetel, Telstra, website hosting, maintenance and analysis plus system support services.
- Council honoraria (\$21k) and expenses (\$90k) are based on the current meeting schedule and approved payments.
- Delegate expenses and training throughout the year have been projected at \$120k.
- Depreciation (non cash item) is anticipated at \$1.3m this financial year based on current asset register and budgeted additions and disposals throughout the year
- Donations include ALP fundraising dinners (\$25k), Foundation House (\$50k), a proposed Women's shelter (\$50k) plus other approved ad hoc donations made throughout the year (\$25k).
- Insurance costs for the year are estimated at \$1.32m which includes the introduction of the approved Emergency Ambulance policy for members from 1 July 2019.

- Legal expenses incurred for the interests of the Union and members are estimated at \$400k.
- Marketing and communications expenses (\$408k) include promotions, Unified magazine, media, merchandise, recruitment initiatives and the member rewards program estimated in the next 12-month period.
- Motor vehicle expenses (\$475k) are based on 41 vehicles in the fleet and increasing by 4 vehicles for the proposed new staffing positions. The replacement program estimates that 12 new vehicles will be required over the period.
- Wages costs are based on proposed staffing levels broken into divisions (\$9.55m) based on the conditions set in the approved EBA. It should be noted that administration includes records, reception, marketing, communications, IT, training, finance, medical liaison officer, executive assistants and chief of staff. There have been 8 additional roles built into the budget for the year (Communications Officer, Executive Support Officer, Assistant Industrial Officer and 5 organising roles for various divisions).
- Associated staffing on-costs are also listed (\$2.36m) including leave provisions, FBT, payroll tax, workers compensation, superannuation, staff uniforms, training & amenities.
- Travel expenditure has been budgeted according to 2019 actual expenses to accommodate the present travel activity by staff (\$450k).

Recommendation That the HSU NSW/ACT/QLD Union Council discuss, review and adopt the budget/cashflow projection for the 2020 financial year.

Author Angela Nigro

**HEALTH SERVICES UNION NSW/ACT/QLD
OPERATING PROFIT AND CASH FLOW PROJECTION
FROM 1 JULY 2019 TO 30 JUNE 2020**

	Actual FY19	Budget FY19	TOTAL FY20	Jul-19	Aug-19	Sep-19	Oct-19	Nov-19	Dec-19	Jan-20	Feb-20	Mar-20	Apr-20	May-20	Jun-20
	\$	\$													
Income															
Membership Contributions	18,355,827	17,792,000	19,060,500	1,434,954	1,793,692	1,434,954	1,727,940	1,545,052	1,455,108	1,844,077	1,475,262	1,475,262	1,705,592	1,593,162	1,496,446
Advertising	14,780	15,200	12,000	-	3,000	-	-	-	3,000	-	-	3,000	-	-	3,000
Interest Received	66,283	55,400	85,000	6,100	7,900	7,900	7,900	7,900	7,900	7,900	7,900	7,900	7,900	7,900	7,900
Rent Received	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
109 Pitt Street Sydney	1,175,024	1,187,112	1,230,874	101,108	96,184	95,409	96,673	102,807	102,950	103,367	104,680	104,680	104,680	104,680	106,376
370 Pitt Street Sydney	44,841	44,420	87,770	4,300	4,350	4,350	4,410	4,410	4,410	4,410	4,410	4,410	4,410	4,410	4,410
Bankomorrow Warehouse	71,610	71,462	6,000	6,000	6,000	6,000	6,188	6,188	6,188	6,188	6,188	6,188	6,188	6,188	6,188
Total Rent Received	1,291,534	1,307,194	1,347,120	111,748	105,581	105,851	107,887	113,405	113,548	113,945	115,278	115,278	115,278	115,278	115,374
Service Fee - NSW Branch	400,000	400,000	340,000	-	-	-	-	-	-	-	-	-	-	-	-
Sponsorship	-	20,000	32,727	-	-	100,000	-	-	-	100,000	-	-	100,000	-	80,000
Sundry Income	12,608	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Surplus on Sale of Fixed Assets	35,141	36,000	60,000	-	-	15,000	-	-	15,000	-	-	15,000	-	-	15,000
Total Income	20,161,145	19,739,794	20,987,377	1,587,252	1,907,154	1,666,721	1,842,081	1,667,357	1,694,255	1,955,362	1,588,440	1,716,440	1,903,770	1,716,440	1,721,320
Expenses															
Affiliation & Subscription Fees	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
General Affiliations & Subscriptions	84,844	85,000	83,000	4,583	4,583	4,583	4,583	4,583	4,583	4,583	4,583	4,583	4,583	4,583	4,583
ALP	173,300	146,660	187,135	15,595	15,595	15,595	15,595	15,595	15,595	15,595	15,595	15,595	15,595	15,595	15,595
ACTU	217,863	228,400	238,876	19,353	19,353	19,353	19,353	19,353	19,353	19,353	20,327	20,327	20,327	20,327	20,327
Unions NSW	131,353	133,230	135,174	11,264	11,264	11,264	11,264	11,264	11,264	11,264	11,264	11,264	11,264	11,264	11,264
Confederation HSU National	723,114	720,810	746,441	63,610	63,610	63,610	63,610	63,610	63,610	63,610	63,610	63,610	63,610	63,610	63,610
Total Affiliation & Subscriptions	1,210,532	1,219,100	1,281,753	114,445	114,445	114,445	114,445	114,445	114,445	115,613	115,613	115,613	115,613	115,613	115,613
Annual Delegates Conference	181,438	250,000	850,000	650,000	-	-	-	-	-	-	-	-	-	-	-
Audit Fees	53,216	54,750	53,250	4,583	4,583	4,583	4,583	4,583	4,583	4,583	4,583	4,583	4,583	4,583	4,583
Bad Debts	185	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Bank Charges	59,273	57,500	60,500	5,042	5,042	5,042	5,042	5,042	5,042	5,042	5,042	5,042	5,042	5,042	5,042
Buildings Costs	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Cleaning & Consumables	45,758	38,400	50,000	4,167	4,167	4,167	4,167	4,167	4,167	4,167	4,167	4,167	4,167	4,167	4,167
Council Rates	68,493	67,500	73,000	6,250	6,250	6,250	6,250	6,250	6,250	6,250	6,250	6,250	6,250	6,250	6,250
Electricity	29,033	34,800	34,000	8,500	8,500	8,500	8,500	8,500	8,500	8,500	8,500	8,500	8,500	8,500	8,500
Land Tax	71,941	69,400	84,000	6,833	6,833	6,833	6,833	6,833	6,833	6,833	6,833	6,833	6,833	6,833	6,833
Management & Commission Fees	35,888	39,000	44,000	4,500	4,500	4,500	4,500	4,500	4,500	4,500	4,500	4,500	4,500	4,500	4,500
Repairs & Maintenance	20,427	20,000	25,000	2,083	2,083	2,083	2,083	2,083	2,083	2,083	2,083	2,083	2,083	2,083	2,083
Security	5,378	5,000	5,000	500	500	500	500	500	500	500	500	500	500	500	500
Strata Fees	416,818	373,500	431,800	37,792	37,792	37,792	37,792	37,792	37,792	37,792	37,792	37,792	37,792	37,792	37,792
Water Rates	1,281	3,000	3,000	750	750	750	750	750	750	750	750	750	750	750	750
Total Buildings Costs	701,574	671,120	733,200	71,375	82,125	82,125	82,125	82,125	82,125	82,125	82,125	82,125	82,125	82,125	82,125
Campaign Expenses	91,307	130,000	150,800	12,500	12,500	12,500	12,500	12,500	12,500	12,500	12,500	12,500	12,500	12,500	12,500
Commission	43	500	500	42	42	42	42	42	42	42	42	42	42	42	42
Computer & IT Expenses	421,238	443,000	394,000	37,000	32,000	32,000	32,000	32,000	32,000	32,000	32,000	32,000	32,000	32,000	32,000
Consultants	81,534	15,000	20,000	1,667	1,667	1,667	1,667	1,667	1,667	1,667	1,667	1,667	1,667	1,667	1,667
Council & BCOM Honoraria	20,160	19,100	21,300	1,700	1,700	1,700	1,700	1,700	1,700	1,700	1,700	1,700	1,700	1,700	1,700
Council & BCOM Expenses	82,810	100,000	90,800	7,500	7,500	7,500	7,500	7,500	7,500	7,500	7,500	7,500	7,500	7,500	7,500
Credit Merchant Fees	88,734	88,000	60,000	5,000	5,000	5,000	5,000	5,000	5,000	5,000	5,000	5,000	5,000	5,000	5,000
Delegate Expenses	86,598	110,000	100,000	8,333	8,333	8,333	8,333	8,333	8,333	8,333	8,333	8,333	8,333	8,333	8,333
Delegate Seminars & Training & Forums	13,552	207,100	20,400	1,667	1,667	1,667	1,667	1,667	1,667	1,667	1,667	1,667	1,667	1,667	1,667
Depreciation	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Land & Buildings	485,904	455,904	485,904	41,268	41,267	39,941	41,268	39,937	41,269	41,267	38,469	41,271	39,937	41,267	38,746
Plant & Equipment	89,830	87,025	109,781	8,330	8,262	8,000	9,567	8,839	9,027	8,874	8,479	10,360	10,114	10,337	9,465
Furniture & Filings	331,718	321,078	363,593	28,595	28,562	28,892	29,888	28,888	31,068	32,314	31,720	34,816	33,694	31,388	28,767
Motor Vehicles	1,218,693	1,351,075	286,239	104,239	104,239	104,239	104,239	104,239	104,239	104,239	104,239	104,239	104,239	104,239	104,239
Total Depreciation	1,218,693	1,351,075	286,239	104,239	104,239	104,239	104,239	104,239	104,239	104,239	104,239	104,239	104,239	104,239	104,239
Donations - Political	342,861	324,898	75,000	2,083	2,083	2,083	2,083	2,083	2,083	2,083	2,083	2,083	2,083	2,083	2,083
Donations	123,164	125,000	127,000	2,083	2,083	2,083	2,083	2,083	2,083	2,083	2,083	2,083	2,083	2,083	2,083
General Expenses	25	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Insurance	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
General Insurance	135,969	131,025	142,254	11,658	11,658	11,658	11,617	11,917	11,917	11,917	11,917	11,917	11,917	11,917	11,917
Member Emergency Ambulance	12,750	73,500	81,000	4,500	4,500	4,500	4,500	4,500	4,500	4,500	4,500	4,500	4,500	4,500	4,500
Member Entertainment	460,143	474,810	493,501	36,667	36,667	36,667	36,667	36,667	36,667	36,667	36,667	36,667	36,667	36,667	36,667
Member Journeys	324,360	330,739	352,188	27,396	27,396	27,396	27,396	27,396	27,396	27,396	27,396	27,396	27,396	27,396	27,396
Member Professional Indemnity	156,474	151,810	162,172	13,017	13,017	13,017	13,017	13,017	13,017	13,017	13,017	13,017	13,017	13,017	13,017
Member Public Liability	23,492	26,353	27,555	2,185	2,185	2,185	2,185	2,185	2,185	2,185	2,185	2,185	2,185	2,185	2,185
Total Insurance	1,145,059	1,149,125	1,320,814	102,438	102,438	102,438	110,167	112,417	112,417	112,417	112,417	112,417	112,417	112,417	112,417
Interest & Line Fees Paid	87,555	75,657	-	-	-	-	-	-	-	-	-	-	-	-	-
Legal Costs	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Business	151,551	40,000	200,000	16,667	16,667	16,667	16,667	16,667	16,667	16,667	16,667	16,667	16,667	16,667	16,667
Members	127,838	200,000	200,000	16,667	16,667	16,667	16,667	16,667	16,667	16,667	16,667	16,667	16,667	16,667	16,667
Total Legal Costs	279,389	240,000	400,000	33,333	33,333	33,333	33,333	33,333	33,333	33,333	33,333	33,333	33,333	33,333	33,333
Loss On Disposal of Assets	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Marketing & Communications	330,305	360,000	408,000	29,000	29,000	29,000	29,000	29,000	29,000	29,000	29,000	29,000	29,000	29,000	29,000
Meal Entertainment	16,360	30,000	24,000	2,000	2,000	2,000	2,000	2,000	2,000	2,000	2,000	2,000	2,000	2,000	2,000
Motor Vehicle Expenses	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Fleet Management Fees	17,459	25,818	21,240	1,395	1,395	2,500	1,395	1,395	2,520	1,395	1,395	2,520	1,395	1,395	2,520
Insurance & Registration	85,428	80,800	89,830	7,200	7,200	7,200	7,200	7,200	7,200	7,200	7,200	7,200	7,200	7,200	7,200
Motorway Tolls	21,357	21,445	2,083	2,083	2,083	2,083	2,083	2,083	2,083	2,083	2,083	2,083	2,083	2,083	2,083
Parking	138,464	139,485	138,000	11,250	11,250	11,250	11,250	11,250	11,250	11,250	11,250	11,250	11,250	11,250	11,250
Petrol	138,512	134,180	144,000	12,083	12,083	12,083	12,083	12,083	12,083	12,083	12,083	12,083	12,083	12,083	12,083
Repairs & Maintenance	33,723	84,500	60,000	5,000	5,000	5,000	5,000	5,000	5,000	5,000	5,000	5,000	5,000	5,000	5,000
Total Motor Vehicle Expenses	443,543	476,076	475,780	39,612	39,										

[illegible]

Insurance Brokerage Services Tender Committee Report

The HSU has recently run an Expression of Interest process for Insurance Brokerage Services. This meets the requirement to market test contracts with external providers every three years.

The HSU's current broker is Coverforce Insurance Brokers. The 2018/19 insurance program (expiring 30 September 2019) includes:

Policy	Cost	Insurer
Association Liability	\$26,361	QBE
Corporate Travel	\$999	Accident & Health
Cyber Liability	\$8,400	Lloyd's Of London
Industrial Special Risks	\$15,369	Vero
ISR – Crime	\$2,868	Vero
Machinery Breakdown	\$3,281	Vero
Motor Vehicle Fleet	\$49,015	QBE
Public Liability	\$8,973	Vero
Voluntary Workers	\$766	Zurich
Bereavement – Members Product	\$464,000	Hannover
Journey – Members Product	\$328,757	AIG
Professional Indemnity – Members Product	\$227,981	Vero
Public Liability – Members Product	\$26,223	Vero
Workers Compensation Services	\$8,000	Ability Group
HSU Broker Fee	\$73,000	Coverforce
TOTAL	\$1,243,995	

The EOI was advertised in the SMH and eight broker companies requests a copy of the EOI document, of which three provided proposals. These were: Marsh, Coverforce and General Insurance Brokers of Australia (GIBA). A comparison table was completed and all three companies were deemed suitable to provide a presentation to a Tender Committee which was made up of managers involved in the insurance program; Lynne Russell (Assistant Secretary/Treasurer), Angela Nigro (Chief Financial Officer) and Ayshe Lewis (Divisional Manager, Industrial).

Overview of presentations held on 24th June 2019

2.00pm Marsh

- Impressive presentation from a large company.
- Marsh had representatives from Sydney, Adelaide and Victoria and gave a very comprehensive overview of what they could offer the HSU and its members.
- Provided a Project Manager to handle transition who was present at the presentation and is based in Sydney.
- Had other union clients in other states and the retention rates of clients were quite high.
- Understood the difficulty of obtaining Association Liability Insurance but gave an undertaking to find this insurance coverage either in Australia or an overseas market.
- Offered additional services that could be purchased if required including an interesting service called a "Discretionary Trust" that HSU could possibly use in the future.
- Cost of this broker was the lowest of the 3 tenders.

2.45pm GIBA

- Another impressive company who gave an informative and professional presentation.
- Had union clients and had retained its customers.
- Senior broker had good knowledge of Unions and had been a former FSU delegate.
- Also understood the difficulty of obtaining Association Liability Insurance but gave an undertaking to find this insurance coverage (would prefer to obtain this from a local group but may have to go overseas).
- Company had huge experience as brokers so vast knowledge of products and services.
- Cost of this broker was the highest of the 3 tenders

3.30pm Coverforce

- Coverforce is our current Insurance broker.
- Very disappointing presentation.
- Presenters were unprepared for questions.
- Questions were asked of the presenter around issues that the HSU and its members were currently experiencing, and the response was to set up a meeting to discuss.
- Tender committee felt that Coverforce had not presented in a professional manner and had taken the HSU for granted and the presentation was more of a catch up rather than the opportunity to “sell” its product to a consumer.
- Large amount of Union clients.
- Coverforce did not have a solution to provide Association Liability Insurance in the first instance however said they could split insurances to cover directors and officers of the union.
- Cost of this broker was midway between the other 2 tenders.

Following the presentations and after considerable discussion, based on the proposals received, pricing, experience and understanding of HSU needs, Marsh was selected by the Tender Committee as the recommended insurance broker of the HSU insurance program for the next three years. This was then endorsed by the Audit & Finance Committee at their June 2019 meeting.

Resolution:

That the HSU NSW/ACT/QLD Union Council approves the engagement of Marsh as the insurance broker of the HSU insurance program to 2022. Further, that the Assistant Secretary/Treasurer is authorised to renew the insurance policies on expiry over the next three years based on advice from Marsh insurance brokers.

HSU Insurance Brokerage Service EOI 2019 Assessment Table

Evaluation Criteria	Marsh	Coverforce	General Insurance Brokers of Australia
<i>Selection Criteria 1.</i> Extent to which interested parties meet the statement of requirement for provision of insurance advice and procurement of insurance policies			
<p>Approach to risk assessment and advice on insurance coverage</p>	<p>Marsh would implement their six step Annual Insurance Cycle Process:</p> <ol style="list-style-type: none"> 1. Understand the business and objectives 2. Design the right insurance program 3. Engage with insurers to negotiate on our behalf 4. Provide options and recommendations 5. Place cover in accordance with our instructions 6. Deliver evidence of insurance cover and arrange payments to insurers 	<p>Coverforce states that as they have worked closely with the HSU for some time they have a keen insight and understanding of the HSU business and where the insurance program can add maximum value. They will assist the HSU by reviewing each contract to ensure that the current programmes adequately address the exposures and risks and give advice where changes are required.</p>	<p>GIBA focuses on intelligent design to balance risk and reward for the organisation. Services include:</p> <ul style="list-style-type: none"> • Business fact find to familiarise themselves with the activities of the Union to identify present and future risks to operation, employees and members. • Establish plan to mitigate and minimise risk exposure by offloading risk to appropriate insurance products. • Compare and audit existing covers to assess if they are fit for purpose. • Provide feedback and advice. • Go to market to procure insurance policies.
<p>Approach to procurement of insurance policies</p>	<p>Their assessment would involve a gap analysis on the existing corporate insurance program and identify emerging risks that may affect the trade union sector.</p> <p>Marsh's strategy includes a process of setting clear timelines and objectives, preparing quality submissions and engaging with the market to achieve the best outcome for the insurance program.</p> <ul style="list-style-type: none"> • Clear structured timeline • Agreement of target objectives • Market identification and segmentation • Development of a high quality risk submission • Insurer engagement and strategy • Final negotiations <p>They work with a number of union and association clients on member benefit products.</p>	<p>The dedicated Account Executive constructs a yearly renewal plan which included such things as claims experience, changes in normal work practices, changes in the market, anticipated future activity and the like. The plan is tabled at a review meeting with the HSU where the Account Executive outlines a recommended series of options and a recommended plan. The meeting considers what steps should be taken including:</p> <ul style="list-style-type: none"> • Changes in programme, incorporating future activity • Are the limits adequate? • What changes can be made to the deductible to improve the overall package • Has the performance of the underwriter(s) been acceptable? if not, what action needs to be taken • Is the policy rating competitive with similar risks? Does it take into account the risk management efforts and claims experience • What alternative underwriters should be approached 	<p>GIBA undertakes a robust process when taking the insurance needs to the market including:</p> <ul style="list-style-type: none"> • Tendering – the broker will manage the end to end process • Presenting findings and make recommendations – prepare a detailed tender pack to HSU stakeholders • Placing insurance – instruct insurer to bind, provide policy workings and certificates of currency • Educating HSU staff – develop and produce a manual which contains procedures and guidelines and will provide training if required • Managing renewals

Selection Criteria 2.			
Extent to which interested parties meet the statement of requirement for administration, management and reporting of insurance policies			
Approach to administration	Marsh commits to the delivery of efficient servicing and includes: 1. Insurance program design and placement 2. Ongoing advice and communication 3. Provision of documentation	Coverforce will be responsible for all aspects of the administration of the policy for the HSU and their members.	A tailored claims report produced each quarter with visibility and detail including: <ul style="list-style-type: none"> • Executive summary • Summary of incidents • Claim type • Claim details • Claims status • Claims outcome • Summary of total claims and values
Approach to claims management	Dedicated Client Executive to handle all general insurance claims. Marsh's role in managing claims: <ul style="list-style-type: none"> • Inform insurers of incident • Provide interface between the HSU and the insurer experts, allowing for information to be exchanged in a timely fashion • Attend and facilitate meetings with insurer's experts • Help maximise claim payment under the policy • Manage transfer claim settlement money A proactive approach to claims management <ul style="list-style-type: none"> • Pre-claim • Notification • Claim • Post loss Marsh state they are a leader in the provision of claims servicing models for member-based programs. They will tailor a website for each program and have an online claims form and a support hotline available for HSU members.	Coverforce has a skilled internal claim teams and will act on behalf of the claimant and not the insurer. They are proactive in finding out the status of claims on behalf of the client. Quarterly reporting in the status of claims and meetings if requested or required.	GIBA will appoint a dedicated Claims Manager to be the first point of contact. They maintain a close working relationship with the underwriters and insurers in order to get the immediate action, assistance and clarity as to how the claim is progressing. They are happy to receive and assist calls and enquires providing assistance to members keeping them informed of next steps.
Selection Criteria 3.			
Previous experience and past performance			
Other clients served by this company	Marsh has for many years has provided general insurance broking services for trade unions, associations, health and not for profit organisations. Union clients include CFMEU (SA, WA & ACT), CEPU (SA), PSA (SA) and United Voice. Other clients include Australian Football League, Cricket Australia, Red Cross, Cancer Council of NSW and over 450 Local Government Schemes.	Coverforce have found that Trade Unions have traditionally not been well understood by Insurance Brokers nor Insurers and wrong types of Insurance have been arranged, with incorrect Limits and using Insurers not suited to the Client. Union clients include Unions NSW, TWU (NSW), CFMEU (NSW), PSA (NSW), FSU (National), CEPU, AMEU (NSW) and AMWU (National). Other clients include the Australian Labor Party, Foundation House and McKell Institute.	GIBA has recently introduced a broker team with extensive experience and highly qualified in providing and administering insurance solutions for their union clients including AWU, ETU, Nurses Association of NSW, Shop Distribution and Allied Services, Flight Attendants Association of Australia, RTBUB and Correctional Services Union.
Organisational details	Marsh is owned by Marsh & McLennan Companies Inc – a global listed professional services firm. They were established in Australia in 1953 with currently 1,700 staff	Coverforce is now the largest unlisted Insurance Broker in Australia and is governed by a Board of Directors. They employ over 150 staff and have offices in Sydney, Melbourne, Brisbane, Adelaide and Perth.	Since 2010 GIBA has provided tailored insurance solutions and risk management advice to businesses. The overall responsibility and decision making lies with the board.

	nationwide and operates from 33 offices located across all states and territories.		Offices located in Sydney, Melbourne and Brisbane with over 20 staff.
Referees provided	Two referees provided (United Voice and CFMEU).	None provided.	None provided.
Selection Criteria 4.			
Management, Governance and Infrastructure			
Servicing Team	Senior Account Executive will be the key point of contact. The team listed in the proposal will ensure that the end-to-end requirements, from the contract transition through to day-to-day management and claims resolutions will be conducted with efficiency and accuracy for all stakeholders.	Coverforce will have a dedicated Service Team available all year round (listed in proposal) to provide expert risk advice, contract reviews and to adapt the insurance program to reflect changes to assets or operations.	GIBA would have a dedicated HSU project team (listed in the proposal). They pride themselves on customer service and encourage and will provide multiple avenues for HSU staff and members to contact including by phone, email and website contact forms.
Registration certificates provided including professional indemnity cover and public liability	Yes	No	Yes
Fees	\$30,000 plus GST annual servicing fee for the HSU Corporate Program <i>* Marsh have stated that any additional member benefits program would be charged on a per member basis and negotiated upon appointment.</i>	\$73,000 plus GST annual servicing fee. <i>* Coverforce have added a note that the final fee to be negotiated with HSU upon formal pricing for the 2019/20 insurance period.</i>	Risk assessment and advice on insurance coverage - \$25,000 Tender management (including procurement of policies) - \$40,000 Administration and management of Insurance Policies and claims - \$40,000 Provision of quarterly reports - \$5,000 Total cost - \$110,000 plus GST
Comments	Marsh's proposal is set out in an easy to follow format in line with the selection criteria provided in the HSU EOI. Separate claim team for the general policies and the member programs. No fee included for the proposed member programs in the proposal. Provided recommendations for potential additional cover the HSU could provide members.	Coverforce has been the HSU's broker for last six years. The service fee listed in the proposal is the same as the last two years. Their proposal is set out in an easy to follow format in line with the selection criteria provided in the HSU EOI document, however criteria 2 was not listed in the proposal and no referees, registration or insurance certificates were provided. The HSU does not receive ongoing quarterly reports on claims unless asked although this request was in the 2016 tender process to be included.	Marsh's proposal is set out in an easy to follow format in line with the selection criteria provided in the HSU EOI, however did not provide referees. The most expensive of the three proposals, however the other 2 proposals have an * with additional or potential additional costs. Have only been in operation since 2010, although was founded by four experienced professionals with over 150 years of insurance broking experience between them. Sydney office is located in the same building as HSU head office (level 11). Provided recommendations for potential additional cover the HSU could provide members.



IT Security Policy

V1.0

Document Information

Document Status	
Version Number:	1.0
Last Update:	Initial policy
Document Title:	IT Security Policy

Version:	Issue Date:	Comments	Approved By:
1.0	14 July 2019	Initial policy implementation	Union Council

This policy is a living document and can be updated as determined by those responsible for updates and revisions. Ad hoc and scheduled reviews should also take place to reflect the changing requirements within the Health Services Union.

All requests for changes can be submitted to the policy owner, whom will discuss change requests with the relevant stakeholders and accept or reject the request. Following approval by Union Council, the change(s) will be incorporated into this policy.

Confidentiality

You should carefully review the following confidentiality condition prior to reading or using this document.

This document contains confidential information of which you may not directly or indirectly use, disclose or publish or permit its use, disclosure or publication without the express written permission of Health Services Union.

Reading or using this document indicates your acceptance of this confidentiality condition. If you do not agree with these terms and conditions, you should promptly return the document to Health Services Union.

This confidentiality condition forms a binding agreement between you and Health Services Union.

Table of Contents

1. Purpose	4
2. Scope.....	4
3. Accountability.....	5
4. Management Roles and Responsibilities.....	5
5. PCI Roles and Responsibilities	6
6. Protection of Information	7
7. IT Security Policy	7
7.1 Staff Induction and Training	7
7.2 Access Controls	8
7.3 Terminating Staff.....	8
7.4 Asset Database and Registers.....	8
7.5 Hardware & Asset Tags	9
7.6 Virus Controls.....	9
7.7 Firewall Configuration	9
7.8 Wireless Environment Controls	10
7.9 Remote Access	11
7.10 System Configuration.....	11
7.11 Server Security.....	12
7.12 Patch Management.....	13
7.13 Logging and Monitoring Controls	13
8. Vulnerability Management.....	14
9. Business Continuity and Disaster Recovery	14
10. Risk Assessment	15
10.1 Risk Assessment – Key Steps	16
10.2 Likelihood Ratings.....	17
10.3 Consequence Ratings.....	17
10.4 Risk Matrix	18
10.5 Risk Ratings.....	18
11. Compliance.....	19
12. Documentation required with this Policy.....	20
13. Glossary.....	21

IT Security Policy

1. Purpose

The Information Technology Security Policy outlines the organisation's requirements to protect *Health Services Union* information in different stages of processing, transmission, or storage. This forms part of the organisation's suite of policies aiming to protect the confidentiality integrity and availability of all *Health Services Union* and our clients' information, especially classified information, such as payment card information.

The intention of this policy is to provide guidelines, for employees to apply personal judgment in their use of *Health Services Union*'s resources to protect its technology, infrastructure and people in order to reduce the exposure of risks to information. Mis-handling of information could occur intentionally or unintentionally, resulting in incidents such as data breaches and impact the integrity of *Health Services Union* and its customers' information, as well as our corporate reputation.

This policy is also designed to adhere to Payment Card Industry (PCI) Data Security Standard (DSS) v3.2 requirements. *Health Services Union* understands that some clients are required to comply with PCI DSS due to transmitting, storing or processing payment card information (e.g. credit card details). Refer to Compliance section for further information.

2. Scope

This policy applies to all officers and staff, including full time and part time employees, contractors, consultants, and other workers at the organisation's offices and customer service sites, including all personnel affiliated with third parties.

This Policy outlines the criteria for easily classifying and protecting *Health Services Union*'s and its members' information resources, particularly with regard to, but not limited, to the following types of information:

- Member information
- Budgets and business plans
- Employees' personal information

The level and type of access for employees located at contact centres may vary depending on the organisation's requirements.

3. Accountability

The following personnel have designated responsibilities to information security management with regard to the requirements in this policy:

Role Title	Accountability
Chief Financial Officer (CFO)	Responsible for ensuring that all <i>Health Services Union</i> information is securely maintained, and compliance requirements are adhered.
Information Technology (IT) Administrator	Responsible for ensuring all systems and monitoring takes place as needed and ensuring that all technical systems are adequately controlled in line with this policy and users are only provisioned access and use as per their role requirements.
Managed Services Provider	Responsible for 2nd tier support and monitoring of servers and all IT related services. Supplying additional support in house when IT administrator on leave.
Human Resources Manager(s)	Responsible for ensuring that all users adhere to this policy and non-compliance or deviation from this policy is managed.
End User(s)	Responsible for following this policy and asking for further clarification if required.
Third Party (ies)	Responsible for being aware of this policy and adhering to it if working on <i>Health Services Union</i> premises and using <i>Health Services Union</i> 's IT resources.
Information Asset Owner	The <i>Health Services Union</i> may choose to allocate information owners whom are responsible for overseeing that information is appropriate classified, accessed and managed.

4. Management Roles and Responsibilities

The Chief Financial Officer is responsible for aiding the IT Administrator in promulgating a set of industry standard compliant security technical standards, including the following:

- Network design, router and firewall configuration standards;
- Server build, hardening and patching standards;
- The establishment of sound user verification and identification policies, ensuring that all actions taken can be traced back to individuals, and that opportunities for unauthorised access to information are minimised;
- The establishment of security monitoring practices, including network intrusion detection, prevention, incident logging, file integrity monitoring and Security Event correlation alerting;
- Methods and practices for the secure storage and transmission of private and confidential data.
- Establishing a program of risk review and mitigation, including internal and external testing of network and systems vulnerabilities;
- Establishing and maintaining a sound change management system;
- Establishing and maintaining an incident response process, which addresses legal, contractual and technical responses to any incident which impacts on the Confidentiality, Availability or Integrity of *Health Services Union* 's information assets.
- A set of processes for managing service providers and vendors in their interaction with *Health Services Union* 's information assets.

5. PCI Roles and Responsibilities

The following information security responsibilities must be specifically and formally assigned:

Responsibility	Individual or Team Assigned
Overseeing and ensuring <i>HEALTH SERVICES UNION</i> maintains a PCI Compliance program which is audited and complied with on an annual basis.	CFO
Ensure an effective security awareness program is in place.	HR
Ensuring <i>Health Services Union's</i> management is adequately informed of their responsibilities with regards to protection of Cardholder Data.	CFO / IT Administrator
Ensuring all new environments are implemented in a manner that complies with the PCI DSS. <i>Health Services Union</i>	IT Administrator / Managed Service Provider
Monitor and analyse security alerts and information and distribute to appropriate personnel.	IT Administrator / Managed Service Provider
Logical management of network components	IT Administrator / Managed Service Provider
Establishing, documenting and distributing security policies and procedures	CFO / IT Administrator / HR
Administration of user accounts, including additions, deletions, modifications and authentication management	IT Administrator
Monitor and control all access to data. Implementing access controls.	IT Administrator

6. Protection of Information

The Health Services Union must have a formal approach to identify and protect the Confidentiality, Integrity and Availability of all its information assets. This will ensure safeguard of its information and that of its clients, the continuity of its operations, minimise the impact of should information security incident occur.

- Implement Information Security framework or strategy based on industry best practices (ISO 27001/2) to ensure secure management of all information across the organisation.
- Ensure that its information security practices is enforceable by all employees by understanding the information asset type, classification and protective measures.
- *Do not* store PAN details under any circumstances on any system, including data system or hard copy. Any evidence of CHD must be destroyed. If PAN is required to be stored, then appropriate encryption methods must be used in line with PCI DSS requirements.
- Implement suitable controls, which consist of people, policies, procedure, standards, guidelines and technologies (hardware and software) to mitigate any exposure to its own or clients' information.
- *Health Services Union* shall measure the effectiveness of its controls through risk assessment (refer to *Health Services Union* 's Information Risk Assessment procedure), vulnerability management, security audits and compliance checks.
- Retention period for assets and data must be determined based on business and regulatory requirements. These should not be retained longer than required.
- For PCI DSS compliance, event logs from anti-virus software should be kept for a year and at least three months is available for immediate analysis;
- Data classification information shall be documented, reviewed, approved and disseminated to all staff. Policy shall include Labelling, Retention, Media Handling and Destruction process and procedures. (refer to policies in separate document).

7. IT Security Policy

7.1 Staff Induction and Training

It is necessary to have formal procedures in place so that access to systems by new staff is carried out in a secure and consistent manner. Procedures for authorising, establishing, and modifying access privileges must be followed, implemented, and maintained. This includes requesting, authorizing, and allowing access in an emergency situation:

- All employees must have successfully passed background checks prior to commencing employment, including where appropriate, credit and criminal history checks.
- All employees must provide written acknowledge that they have read and understood the Information Security policy and relevant procedures. Requiring an acknowledgement by personnel in writing or electronically helps ensure that they have read and understood the security policies/procedures, and that they have made and will continue to make a commitment to comply with these policies.
- Formal authorisation forms must be completed and signed by the new staff member and their Department Manager. These forms must also be authorised by the IT Administrator, before access will be provided.
- The Human Resources Department will ensure that new staff are given appropriate Information Security education and awareness training prior to access being granted to systems and information.
- Employees must undergo security awareness training including cardholder data security on commencement at *Health Services Union* and at least annually. It may be computer based, team meeting, quiz etc. This must specifically cover compliance requirements such as PCI DSS.
- Appropriate training will be also be provided annually to staff with security breach responsibilities. All personnel must formally acknowledge that they have read and understood the security policy and procedures at least annually. Attendance of training and awareness programs should be maintained

by HR team to ensure refresher trainings are undertaken on an annual basis.

- Staff changing functions or requiring changes to their access privileges must complete a new Staff Access Form via CFO before IT will make changes

7.2 Access Controls

- Strict Policy on General Access Controls must be followed as below:
 - Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following:
 - Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities.
 - Assign access based on individual personnel's job classification and function.
 - Require documented approval by authorized parties specifying required privileges.
 - Restrict access based on a user's need to know, and control is set to "deny all" unless specifically allowed. This access control system must include the following:
 - Coverage of all system components
 - Assignment of privileges to individuals based on job classification and function
 - Default "deny-all" setting

7.3 Terminating Staff

- Terminated staff will have authorisation and access privileges revoked promptly.
- Application owners are responsible for reviewing the Staff Movements notification generated by the exiting staff member's Department Manager. IT will be responsible for removing access by relevant users to the systems.
- IT will be notified immediately of the termination of a user deemed to be a security risk. Their access will be revoked immediately.

7.4 Asset Database and Registers

7.4.1 Software List

- Only software intended, approved and correctly licensed for *Health Services Union's* business goals may be installed or used on any *Health Services Union's* computing device.
- A List or a Register of Approved Products and correctly licensed Software permitted for use within *Health Services Union* must be maintained, periodically reviewed and updated. Responsibility must be explicitly assigned.
- Owners must at a minimum:
 - Determine the sensitivity and/or criticality of the product/software/Operating System under their control
 - Check that the appropriate protection measures are in place
 - Authorise and periodically review access rights to their software and applications
 - Facilitate the resolution of security-related audit issues
 - Periodically review the risk classifications of application software under their control
 - Maintain an inventory of software under their control which should contain personnel information authorised to use the devices.
- List of software running on the server shall include operating system, programs, and services running on the server.

7.4.2 Hardware List

- IT will maintain an accurate and up to date register of all *Health Services Union* IT equipment. This

includes listing of all routers and firewalls, along with the access controls provided by each device.

- Remote Access and Remote-Control solutions used to access systems must be on the approved security solution list.
- Only *Health Services Union* IT staff are authorised to configure, set up and build hardware within the *Health Services Union* business environment consequently only IT staff are authorised to install/uninstall software within the *Health Services Union* IT standard operating environment and remote organisers have rights to install approved application they need.

7.5 Hardware & Asset Tags

- All mobile phones, computers, laptops and desktops will be marked with a unique Health Services Union asset tag.
- All Health Services Union's computer and communications equipment must have a unique identifier ie serial number / asset tag to it such that physical inventories can be efficiently and regularly conducted.
- Labelling should include information such as owner, contact information, and purpose which is included in the Asset register with IT.

7.6 Virus Controls

- Current, up to date anti-virus software will be installed and used on all computers. All anti-virus software must be active regularly updated and capable of generating audit logs.
- Approved malicious code detection software must be installed and utilised: on all vulnerable devices, including but not limited to personal computers, mobile phones, and PDAs at e-mail gateways and messaging servers.
- *Health Services Union* systems must have Anti-Virus, Anti-Spyware and Host Intrusion Prevention modules installed, where required, to provide coverage for different threat vectors.
- Malicious code detection software and signature files must be:
 - maintained at latest vendor levels,
 - configured to monitor and intercept malicious code in real time,
 - configured using the established global anti-virus software configuration
 - For any systems in the PCI DSS environment the Antivirus event logs should be kept for a year with 3 months available online for analysis.

7.7 Firewall Configuration

PCI DSS requires that Firewall and configuration standards must be established and implemented to protect cardholder data. The *Health Services Union's* Firewall configuration standards below must be implemented and followed:

- All network connections and changes to the firewall and router configurations must be formally submitted via proper change process, tested reviewed and approved by authorised personnel. Changes to configuration settings and rules for routers, switches, IDS/IPS and firewall devices shall be confirmed as meeting the business and security objectives before releasing the change into Production status.
- Network diagram showing cardholder data flows over the network must document all connections to cardholder data, including any wireless networks and must be maintained, reviewed and kept current.
- Firewall configuration standards must require that a firewall be implemented and installed:
 - At each Internet connection.
 - Description of groups, roles, and responsibilities for management of network components must be updated and kept current
 - Use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure must be in place and business justification for use of those services and protocols is provided.
 - Routers, switches, firewalls and IPS/IDS capabilities shall be employed to enable network segregation,

traffic flow control and auditing of network events.

- Firewalls and appropriate network address allocations shall be used to facilitate security zones and need to know access according to industry standards and PCI DSS requirements.
- Firewall and router configurations must restrict connections between untrusted networks and any system components in the cardholder data environment.
- Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic
- Perimeter firewalls installed between any wireless networks and systems that store cardholder data, deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment. Secure and synchronize router configuration files.
- Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet. Direct access between publicly accessible environments and the cardholder environment must be prohibited. This applies to both inbound and outbound traffic.
- Traffic must not be allowed to cross the firewall unless explicitly permitted. Filtering of traffic to control and restrict access across the perimeter between the corporate intranet and the public Internet or other untrusted networks must be utilized. This filtering includes, but is not limited to, destination and source IP addresses, ports, applications, and protocols. Network Address Translation (NAT) NAT technologies must be used to mask internal IP addresses and only display an external IP address.
- IP addresses for the private intranet must not be propagated into any untrusted network unless necessary to ensure connectivity and availability
- Settings and rules that are identified as no longer meeting *Health Services Union* 's business objectives shall be revised, deleted or disabled.
- After configuration of routers and firewalls, the running and start-up configurations must be synchronised, and checksums compared to ensure that following a re-boot the running configuration is restored as approved. Backup copies of configuration settings and rules for IDS/IPS and firewall devices shall be maintained.
- Configuration settings and rules for routers, switches, IDS/IPS and firewall devices shall be reviewed at least six months.
- The minimum requirements for configuration settings and rules for routers, switches, IDS/IPS and firewall devices shall be documented, including permitted protocols, services, source and destination addresses etc. shall be reviewed and updated at least annually or when significant changes occur.
- Listing of all routers, along with the access controls provided by each router, must be maintained.

7.8 Wireless Environment Controls

- Firmware of wireless devices must be updated to support strong encryption for authentication and transmission over wireless networks and updated from time to time as recommended by the equipment vendor to retain a secure status. Communications used to remotely manage security functions or devices that provide security controls must be encrypted and authenticated before transmission.
- All security-related vendor defaults for wireless devices must be changed prior to use.
- Vendor supplied default passwords and PINs must be changed prior to implementation into a production environment
- All electronic connections to or from third parties must undergo pre-production connection testing and security assessment. Production use must not occur unless acceptable test results have been obtained.
- The community strings for SNMP must be changed from the vendor defaults.
- Documented inventory records of authorised wireless access points must be maintained, and a business justification is documented for all authorized wireless access points.
- Scanning either before the system is implemented for its intended purpose as a part of the infrastructure or whenever a potential intrusion is identified must be performed and reviewed at least twice a year on all networks, sub-networks and individual machines that are connected to the enterprise.
- Policy must include notification requirement to alert appropriate personnel if automated monitoring is employed for the detection of unauthorised wireless access points.

7.9 Remote Access

- Remote Access and Remote-Control solutions used to access systems must be on the approved security solution list.
- Only approved security devices, such as firewalls, VPN, IDS and IPS, are authorised to be implemented within the *Health Services Union* 's environment. All such devices must be configured in a manner to protect against the circumvention, subversion, or undermining of the required level of security in accordance with industry accepted standards.
- Requests for access to the network through remote access services must be approved by an appropriate level of management
- The ability to copy, move, and store cardholder data onto local hard drives and removable electronic media must be prohibited via remote access technologies.
- Usage policies and proper use of critical technologies shall include remote access and wireless technologies, laptops, tablets, removable electronic media, e-mail usage and Internet usage.

7.9.1 Third Party Remote Access

- All electronic connections to or from third parties must undergo pre-production connection testing and security assessment. Production use must not occur unless acceptable test results have been obtained.
- Remote access for third parties must only be enabled during the time period needed and deactivated immediately after use.
- Remote access sessions must be automatically disconnected after a specific period of inactivity.
- IDs used by vendors to access, support, or maintain system components via remote access will be managed as follows:
 - Monitored when in use.
 - Repeated access attempts will be limited by locking out the user ID after not more than six attempts.
 - Lockout duration will be set to a minimum of 45 minutes or until an administrator enables the user ID.
 - Remote access will be deactivated or removed from the access list for users that has been terminated.

7.10 System Configuration

All policies listed below are to comply with PCI DSS requirement 2.2:

- Develop configuration standards for all system components and ensure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards
- All *Health Services Union* computers, devices and applications shall be configured and hardened to meet the intent of this policy and industry standards.
- A Configuration Standard policy should define how system components are configured to the particular function that is required. Document should show services and port enabled / disabled, list what accounts and password types should be created; or can be very detailed and list step by step how to setup a system component. However, the document should be in line with industry accepted hardening standards and should include instructions for testing that the required hardening has been achieved.
- No changes to any configuration setting on computers, devices and applications are permitted without first having been approved according to *Health Services Union*'s Change Management Procedures. This includes workstations, laptops and similar.
- Approved configurations must be followed to configure remote access services. All *Health Services Union* computers, devices and applications shall be configured and hardened to meet the intent of this policy and industry standards.
- Application or system services not being used for a defined business purpose must be disabled, including any part of the operating system that is unnecessary to the business purpose of the system. (E.g. daemons, "insecure" protocols). If ports, services, daemons, or protocols that are considered "insecure" are being used they need to be justified and security features need to be documented. Additionally, an evidence of security features and controls implemented to mitigate the associated risks

must be provided.)

- That common security parameters settings are included and are set appropriately.

7.11 Server Security

This policy is to set out required minimal security configuration for all server equipment connecting to a production network or used in a production capacity at or on behalf of the *Health Services Union*.

All internal servers deployed are owned by the *Health Services Union* IT Department / Managed Service Provider who are responsible for system administration. Approved server configuration guides which comply with general industry accepted standards (CIS, NIST) must be established and maintained by each operational team, based on business needs and approved by *Health Services Union* IT. The IT teams will monitor configuration compliance and implement an exception policy tailored to their environment. Each IT team must adhere to the IT Department process for changing the configuration guides, which includes review and approval by IT Management.

At a minimum, the following information is required to positively identify the point of contact:

- Server contact(s) and location, and a backup contact.
- Hardware and Operating System/Version.
- Main functions and applications, if applicable.
- Information in the corporate enterprise management system must be kept up-to-date.
- List of software running on the server including operating system, programs, and services running on the server.
- Configuration information about how the server is configured including:
 - Event logging settings
 - A comprehensive list of services that are running.
 - Configuration of any security lockdown tool or setting
 - Account settings
 - Configuration and settings of software running on the server.
- Types of data stored on the server.
- The owners of the data stored on the server.
- The sensitivity of data stored on the server.
- Data on the server that should be backed up along with its location.
- Users or groups with access to data stored on the server.
- Administrators on the server with a list of rights of each administrator.
- The authentication process and protocols used for authentication for users of data on the server.
- The authentication process and protocols used for authentication for administrators on the server.
- Data encryption requirements.
- Authentication encryption requirements.
- List of users accessing data from remote locations and type of media they access data through such as internet or private network.
- List of administrators administrating the server from remote locations and type of media they access the server through such as internet or private network.
- Intrusion detection and prevention method used on the server.
- Latest patch to operating system and each service running.
- Groups or individuals with physical access to the area the server is in and the type of access, such as key or card access.
- Emergency recovery disk and date of last update.

- Disaster recovery plan and location of backup data.
- Configuration changes for production servers must follow the appropriate change management procedures.
 - Operating System configuration should be in accordance with approved IT guidelines.
 - Services and applications that will not be used must be disabled where practical.
 - Access to services should be logged and/or protected through access-control methods such as TCP Wrappers, if possible.

7.12 Patch Management

- The most recent security patches must be installed on the system as soon as practical, the only exception being when immediate application would interfere with business requirements.
- Security patches or mitigation measures must only be communicated and delivered through approved *Health Services Union* processes. Patches or mitigation measures must be reviewed for impact and applicability to the environment and, if appropriate, applied using standard change control procedures. High severity security patches must be installed within 1 month of release.
- Maintain current knowledge of available patches by keeping up with vendor releases and updates.
- Decide what patches are appropriate for particular systems by identifying and assessing the impact of system vulnerabilities and likelihood of exploits eventuating.
- Ensure that patches are installed properly to mitigate system vulnerabilities by testing the patches on test systems prior to installation.
- Verify systems after the installation of patches to ensure successful patch implementation and the vulnerability is no longer present.
- Document all associated procedures and ensuring the procedural steps and roles and responsibilities are kept current.
- Patches are to be tested and evaluated for negative system impact and risk. The vulnerability mitigated by the patch will be evaluated against the impact to business, such as loss of business functionality or operations, other potential vulnerabilities introduced by applying the patch, and availability of system resources.

7.13 Logging and Monitoring Controls

Logging mechanisms and the ability to track user activities are critical in preventing, detecting, or minimizing the impact of a data compromise. The presence of logs in all environments allows thorough tracking, alerting, and analysis when something does go wrong. Determining the cause of a compromise is very difficult, if not impossible, without system activity logs.

It is critical to have a process or system that links user access to system components accessed. This system generates audit logs and provides the ability to trace back suspicious activity to a specific user.

PCI DSS requirement 10 lists the following which must be followed:

- Implement audit trails to link all access to system components to each individual user.
- Implement automated audit trails for all system components to reconstruct the following events:
 - All actions taken by any individual with root or administrative privileges
 - Access to all audit trails.
 - Invalid logical access attempts.
- Use of and changes to identification and authentication mechanisms—including but not limited to creation of new accounts and elevation of privileges—and all changes, additions, or deletions to accounts with root or administrative privileges.
- Initialization, stopping, or pausing of the audit logs.
- Creation and deletion of system-level objects.
- Record at least the following audit trail entries for all system components for each event:

- Using time synchronization technology, synchronize all critical system clocks and times and ensure that the following is implemented for acquiring, distributing, and storing time.

Note: One example of time synchronization technology is Network Time Protocol (NTP). "Critical systems have the correct and consistent time"

- Time data is protected.
- Time settings are received from industry-accepted time sources.
- Secure audit trails so they cannot be altered.
- Limit viewing of audit trails to those with a job-related need.
- Promptly back up audit trail files to a centralized log server or media that is difficult to alter.
- Write logs for external-facing technologies onto a secure, centralized, internal log server or media device.
- Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).
- Review logs and security events for all system components to identify anomalies or suspicious activity. Note: Log harvesting, parsing, and alerting tools may be used to meet this Requirement. "
- Review logs of all other system components periodically based on the organization's policies and risk management strategy, as determined by the organization's annual risk assessment.
- Review logs of all other system components periodically based on the organization's policies and risk management strategy, as determined by the organization's annual risk assessment.
- Follow up exceptions and anomalies identified during the review process.
- Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from back-up).
- Ensure that security policies and operational procedures for monitoring all access to network resources and cardholder data are documented, in use, and known to all affected parties.

8. Vulnerability Management

A vulnerability scan is an automated tool run against external and internal network devices and servers, designed to expose potential vulnerabilities that could be found and exploited by malicious individuals.

There are 2 types of vulnerability scanning required for PCI DSS:

- External month vulnerability scanning, which must be performed by an ASV on Firewall
- Internal and external scanning as needed once a year. Once these weaknesses are identified, the entity corrects them and repeats the scan until all vulnerabilities have been corrected.

Identifying and addressing vulnerabilities in a timely manner reduces the likelihood of a vulnerability being exploited and potential compromise of a system component or cardholder data.

The *Health Services Union* shall run internal and external network vulnerability scans at least yearly.

9. Business Continuity and Disaster Recovery

- The organisation must have a Business Continuity (BCP) and Disaster Recovery (DR) practices in place to ensure its services are uninterrupted and continuously available.
 - Ensure that its client services are uninterrupted, and the availability of services outlined in client contracts is met.
 - Adequate BCP and DR plans should be documented and tested on an annual basis when required.
 - BCP and DR plans of its own network environment must exist and ensure employees are able to perform their business duties efficiently.

10. Risk Assessment

- Ensure all non-compliances, deviations, exposures and gaps are identified and managed as risks.
- Identify and assess risks as per Risk Assessment procedure. A risk assessment must occur least annually to identify threats and vulnerabilities.
- Ensure high and extreme risks are treated as a priority.
- Ensure where feasible, compensating controls are implemented.

Below is the standard Risk Management Cycle as described in ISO 31000:2009 and ISO 27001:2011. This encompasses many phases which aim to provide consistent assessments with comparable and repeatable results.

10.1 Risk Assessment – Key Steps

Figure 1 highlights the key steps in an information security risk assessment process. At a high level, this includes the identification of the risk, assessment and treatment, as well the communication and ongoing review and assessment of risks.

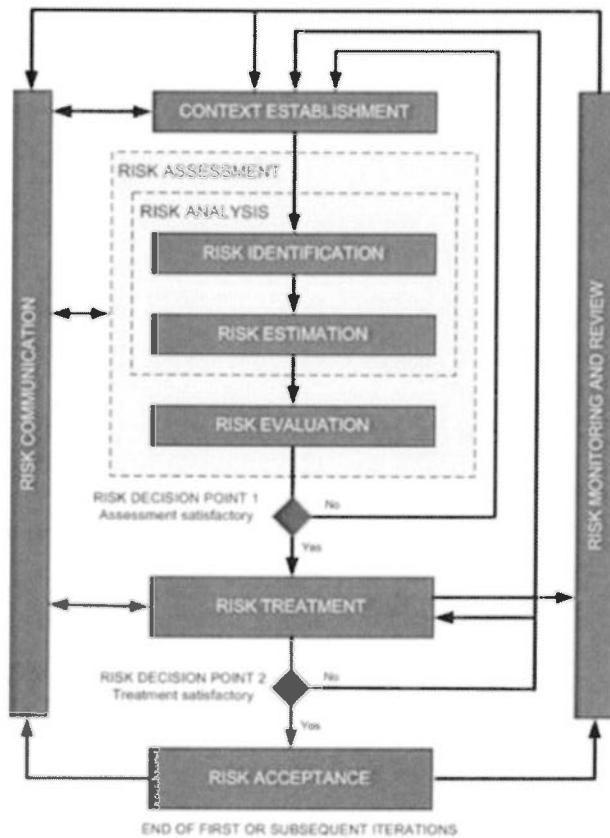


Figure 1: Information risk assessment procedure

10.2 Likelihood Ratings

Likelihood Ratings	Rating #	Description
Almost Certain	5	The event will occur within the next 12 months.
Likely	4	The event will probably occur within the next 12 months.
Moderate	3	The event might occur over the next 12 months.
Unlikely	2	The event could occur sometime in the next 12-24 months.
Rare	1	The event may only occur in exceptional circumstances

10.3 Consequence Ratings

Impact Rating	Rating #	Confidentiality, Integrity, Availability
Very High	5	Loss of sensitive information International reputation impact. Monetary loss (\$1m+)
Major	4	Loss of some sensitive information. National media impact. Monetary loss (\$500k to \$ 1m)
Moderate	3	Loss of some sensitive information. Moderate National media impact (a few occurrences) Monetary loss (\$250k-\$500k)
Minor	2	Loss of some sensitive information. Some National media impact (one occurrence) Monetary loss (\$50k-\$250k)
Insignificant	1	Loss of some sensitive information. Nil media coverage. Monetary loss (less than \$50k)

10.4 Risk Matrix

IMPACT					
LIKELIHOOD	Insignificant	Minor	Moderate	Major	Very High
	1	2	3	4	5
Almost Certain	Low	Medium	High	Critical	Critical
5	-5	-10	-15	-20	-25
Likely	Low	Medium	High	High	Critical
4	-4	-8	-12	-16	-20
Moderate	Informational	Low	Medium	High	High
3	-3	-6	-9	-12	-15
Unlikely	Informational	Low	Low	Medium	Medium
2	-2	-4	-6	-8	-10
Rare	Informational	Informational	Informational	Low	Low
1	-1	-2	-3	-4	-5

10.5 Risk Ratings

Risk Ratings		
Score	Risk	Action
1 – 3	Informational	Report to the IT Security and Risk Officer to add the risk to the Risk Register and reassess annually.
4 – 7	Low	Report to the IT Security and Risk Officer to add the risk to the Risk Register and treat within 6 Monthly
8 – 11	Medium	Report to the IT Security and Risk Officer to add the risk to the Risk Register and treat within 3 Months
12 – 19	High	Report to the IT Security and Risk Officer to add the risk to the Risk Register and treat within 1 Month
20 – 25	Critical	The risk is outstanding and threatens the whole of the operations. It must be reported immediately to the senior management and treated immediately.

11. Compliance

All *Health Services Union* officers and personnel, including full-time, temporary and third-party employees, with access to IT resources must adhere to this policy. The *Health Services Union* undertakes monitoring of IT resources. Deviation from this policy may be permitted with advanced approval in writing by Human Resources Manager.

It is a requirement that all staff have read, understood and agree to abide by this policy and all other Security Policies as a condition of employment. Staff will be asked to sign a copy of each of these documents before access is granted. For existing staff who already have access to these services, you will be provided with a timeframe for reading these documents and asked to sign a copy and return to the IT Department. This signed document will serve as an acknowledgement that you have read the Policy and Guidelines and agree to abide by them.

Employees found to have violated this policy will be disciplined as per *Health Services Union's* Human Resources policies. Corrective actions could include, but are not limited to:

- revoking or restricting any right to use IT systems and equipment, such as email or Internet;
- corrective action, warning or cautioning; or
- Termination of employment.

If employees' behaviour constitutes a criminal offence, then appropriate legal action may be taken. Breaches to this policy can be reported to Human Resources Manager in writing.

Third parties found to have violated this policy may be subject to financial penalties, up to and including termination of contract.

12. Documentation required with this Policy

Documentation	Description
Wireless Access Point Register	Documented inventory records of authorized wireless access points must be maintained, and a business justification is documented for all authorized wireless access points.
Software List	<p>A List or a Register of Approved Products and correctly licensed Software permitted for use within the <i>Health Services Union</i></p> <p>List of software running on server shall include operating system, programs, and services running on the server.</p>
Hardware List, Network, Router, Server List	An up to date register of all IT equipment. This includes listing of all routers, along with the access controls provided by each router, be maintained.
Data Center and Storage	<p>All computer hardware and associated peripheral equipment will be marked with a unique asset tag.</p> <p>Labelling should include information such as owner, contact information, and purpose.</p>
Configuration Settings	<p>The minimum requirements for configuration settings and rules for routers, switches, IDS/IPS and firewall devices is required to be documented, including permitted protocols, services, source and destination addresses etc. shall be reviewed and updated at least annually or when significant changes occur.</p> <p>Listing of all routers, along with the access controls provided by each router, must be maintained.</p>
Data Classification	Data classification information shall be documented, reviewed, approved and disseminated to all staff. Policy shall include Labelling, Retention, Media Handling and Destruction process and procedures
Network Diagrams	Network diagram showing cardholder data flows over the network must document all connections to cardholder data, including any wireless networks and must be maintained, reviewed and kept current.
System Configuration Standards	<p>Document System Configuration Standards for all system components that are consistent with industry accepted System Hardening Standards.</p> <p>A Configuration Standard policy should define how system components are configured to the particular function that is required. Document should show services and port enabled / disabled, list what accounts and password types should be created; or can be very detailed and list step by step how to setup a system component. However, the document should be in line with industry accepted hardening standards and should include instructions for testing that the required hardening has been achieved.</p>
Business Justification for enabled services	Application or system services not being used for a defined business purpose must be disabled, including any part of the operating system that is unnecessary to the business purpose of the system. (E.g. daemons, "insecure" protocols). If ports, services, daemons, or protocols that are considered "insecure" are being used they need to be justified and security features need to be documented. Additionally, an evidence of security features and controls implemented to mitigate the associated risks must be provided.)
Patch Management	All associated procedures and procedural steps and roles and responsibilities for Patch Management.

Roles requiring Access to display of PANs	A list of roles that need access to display of full PAN must be maintained and documented, together with a legitimate business need for each role to have such access.
---	--

13. Glossary

Term	Definition
Cardholder Data (CHD)	<p>At a minimum, cardholder data contains the full primary account number (PAN). Cardholder data may also appear in the form of the full PAN plus any of the following:</p> <p>Cardholder name</p> <p>Expiration date</p> <p>Service Code</p> <p>Full magnetic stripe data (track data) – This information is considered sensitive and must never be stored, even if encrypted</p> <p>CID/CAV2/CVC2/CVV2 (see definition below) – This information is considered sensitive and must never be stored, even if encrypted</p> <p>Pin/Pin Block – This information is considered sensitive and must never be stored, even if encrypted</p>
Cardholder Data Environment	A specific computer system network that stores, processes or transmits cardholder data or sensitive authentication data, and those systems and segments that directly attach or support this environment without segregation controls.
Payment Card Industry (PCI) Data Security Standard (DSS)	Industry standard outlining twelve security requirements applicable to organisations that store, process or transmit payment card information.
Service Code	Three- or four-digit value on the magnetic stripe used for Payment Card Industry purposes.
Users	The term Users refers to all <i>Health Services Union</i> employees, volunteers, contractors and authorised individuals who use or have access to any of <i>Health Services Union</i> information systems, data (regardless of media or form) and physical premises.

Customer Relationship Management (CRM) Program Business Paper

In line with HSU Policy on tendering and procurement, the Customer Relationship Management (CRM) software database was put out to the market via the SMH and Tenderlink. The current contract with Cotswold Concepts (Memforce) expires in October 2019. In order to give sufficient time to transition if that was the decision of the HSU, the tender process commenced in August 2018.

Eleven responses were received and reviewed, a comparison table of the various proposals is attached. Union Council is now required to make a decision based on the recommendation from the Tender Committee as to whether the HSU continues with its existing CRM program or transitions to a new one.

Background: The CRM program manages the HSU database of members' records and also manages payment transactions and case notes for member inquiries. It is a central database platform which underpins much of the work of the HSU – organising, case notes (from industrial/MSD), processing of members fees payments, workplaces, reporting.

The HSU has used Memforce for the last 15 years. This is a customised version of a widely used program called Salesforce and is administered by Cotswold Concepts.

Of the eleven proposals received, six respondents were shortlisted. Five proposals were eliminated based on failure to meet technical requirements or lack of information in the proposal submitted.

A Tender Committee was put together with management and super users representing each division. They convened to review the proposals and hear presentations from the shortlisted companies. Following this, three further proposals were eliminated by a unanimous decision for reasons of failing to meet requirements, technical issues, not meeting HSU needs, excessive cost, expected difficulties in transition and failing to impress the Tender Committee.

This left three top respondents:

APT (Stratum Hawke)

APT is an international British company that initially developed software for the public-sector union in the UK, but has since expanded internationally including Australia. The system is capable of delivering the program needed by the HSU. With many new features and simpler user interface, the company also appears to be geared towards serving unions' very specific and unique requirements (including HSU Vic 2 transitioning to this program recently). This was in contrast to other companies that deliver CRM programs that are meant for selling products to a large customer base, but don't require those customers to have any relationship with each other. A union requires far more interaction between the members on the database as well as grouping them together into workplaces or sub branches, getting them active, delivering training and benefits and getting them organised.

The APT proposal contains the following features:

- Easy to use and easy search capabilities
- User Interface can be easily configured for each individual User, to see only the information they need to see, called "My Page"
- Mobile Access
- Telephone Call Scripting that allows set procedures to pop up when a member calls about a particular issue
- Organises multiple and complex types of relationships into one system

- Events management
- Managing training accreditations of delegates
- Campaign Management module
- Easy to configure reporting
- Dashboards that can be configured to the needs of the User
- Mobile App that shows a Member's financial status
- Efficient and fast credit card payments processing
- Connects with Stripe payments gateway

Implementation cost - \$250,000

Ongoing Cost/annum - \$61,490

Total over 3 years - \$434,470

Cost per user: \$4,345

ASI (iMIS20)

Advanced Solutions International (ASI) is large global company, which specialises in developing software for not-for-profit organisations and other member-based organisations. Their database product is called iMIS, which integrates a website, membership database and communications tools into a single product. They have extensive experience with unions, not-for-profits and member-based organisations.

The key benefits of iMIS is that it would replace a variety of systems into one product. iMIS would essentially become our website, membership database and mass-emailing tool (replacing MailChimp), becoming more than a CRM. It has additional benefits such as "engagement tracking" for individual members (meaning that if a member completes an action such as opening an email, signing a petition, posting on Facebook, etc. the system will automatically increase their score). This is an effective, efficient way of identifying new activists and offline actions (attending a rally, mass-meeting, etc.) can be manually added to their record to improve engagement scores. Other union are building modules and on selling them as a collaborative approach. There has been discussion with ASI about a proposed agreement with the ACTU that would reduce the license fee by paying a fee per member rather than per licence which would reduce the overall cost by around 15%.

Implementation cost - \$300,000

Ongoing Cost/annum - \$182,232 (average as built in CPI increases)

Total over 3 years - \$846,696

Cost per user: \$8,467

Cotswold (Memforce)

Following the presentations of the alternative CRM programs, a comparison was made with the current Memforce Program to consider the many unused features of Memforce and assess whether those under-utilised features could match the APT and ASI proposals. Some new features that can be built into Memforce were also displayed. Cotswold demonstrated that Memforce could provide the following features:

- Reports that can be configured to different groups of HSU users
- Mobile access
- Organises multiple and complex types of relationships into one system – work classifications, workplaces, sub branches, divisions
- Attach documents to Member's records
- "Memforce Touch" which configures Memforce to mobile devices
- Campaign Management enabling mass emailing
- Organiser tools such as mobile access, reports, customised viewing pages
- Tracks member training
- Enterprise agreement and awards register
- Dashboards that can be configured to the needs of the user
- Customisable user interface to make the information easier to see
- Connects with eWay payment gateway for credit card and direct debit processing
- Membership fees management

Some of these features are available now and require some work on configuration to enable use. Memforce will also require some re-training for most staff, as well as the production of User Manuals, as many staff are not using Memforce to its full capacity. The implementation of these new features, along with training for staff on getting the most out of the existing features, is a project that may take up to a year.

Implementation cost – n/a

Ongoing Cost/annum - \$98,712

Total over 3 years - \$296,136

Cost per user: \$2,961

Following the review of the systems it was resolved that Memforce be given a further 6 months to configure, implement and roll out additional feature adoptions to the system to enable staff to get the most out of the program. Following this a re-assessment would take place to determine if this program should be continued or if a change of systems was the preferred recommendation. Cotswold Concepts gave an undertaking that the HSU could extend the current contract for a further 12 months to facilitate the required transition timing. This extension has now passed and a final decision needs to be made.

Options

1. Transition to a new system

The HSU invests in a 14 month process to transition to a new CRM system with a capital outlay, ongoing licence costs (over 3 years) and internal project management costs. Approximate total costs for each proposed systems:

APT (Stratum Hawke) - **\$578,470**

ASI (IMiS) - **\$990,696**

Implementation Process

Any new system implementation will involve the following phases:

- a. Requirements Gathering and Detailed Design

- b. Software Configuration/Development and Prototype Demonstrations
- c. Final Design
- d. Testing
- e. Training
- f. Data Migration
- g. Cutover or 'Go Live' where you switch over from one system to another

These stages involve both additional upfront capital costs to the HSU as well as risk of losing key data during transition, delays in implementation, significant organisational change or not meeting expectations. The HSU would be required to have a dedicated internal staffing or consultant resource to manage the project for all aspects to ensure the smoothest transition possible.

2. Re-sign with Memforce

The HSU re-signs with Cotswold Concepts (Memforce) and in addition invests in an internal resource in the form of a Business Analyst to centralise, prioritise and co-ordinate a number of aspects of the Memforce system to obtain maximum benefit. This includes:

- Greater user awareness of capabilities
- Greater use of reporting facilities
- Customised use of new user interface to departmental requirements
- Department training / workshops centred around capabilities
- Eliminate the use of external spreadsheets where the purpose can be handed within systems
- Integrate Memforce with other 3rd party applications in order to gain greater digital engagement with members including the website, mass emailing, membership benefits etc

Additional Memforce consultant resources to be engaged as required if a project requires a timeline or resources not feasible within the proposed contract including the standard schedule of works.

Costs for this option including Memforce and an internal HSU position of Business Analyst over 3 years - **\$584,136**

Recommendation

After much deliberation, discussion with relevant stakeholders, analysis and risk assessment of the options presented it was resolved that the recommendation to Union Council is to re-sign a three year contract with Cotswold Concepts (Memforce system) and add an internal FTE position of Business Analyst into the staffing structure. This was then endorsed by the Audit & Finance Committee.

The HSU Business Analyst could provide analysis of organisational data to drive optimum outcomes in all areas of the union, not just the membership system. This role would support the development, implementation and management of sophisticated and scalable systems across the union including research, data analysis, and modelling which would assist in deeper integration and future-proofing the HSU with a technology risk management strategy. A proposed draft position description is attached.

Resolution

That the Union Council endorses the recommendation of the Audit & Finance Committee to re-engage Cotswold Concepts. That the Assistant Secretary/Treasurer is approved to sign the contract for the Memforce system for a further three years to 2022. Further that an internal FTE position of Business Analyst be adopted into the HSU staffing structure and recruited for immediately.